Overheden over internationalisering en ICT-recht

Koops, E.J.; Prins, J.E.J.; Schellekens, M.H.M.; Gijrath, S.J.H.; Schreuders, E.

Publication date:
2000

Overheden over internationalisering en ICT-recht

De standpunten van Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten

Bert-Jaap Koops
Corien Prins
Maurice Schellekens
Serge Gijrath
Eric Schreuders

m.m.v. Tomas Oudejans

Centrum voor Recht, Bestuur en Informatisering
Katholieke Universiteit Brabant
mei 2000

Verantwoording

Deze studie is gemaakt in opdracht en met financiële steun van het Ministerie van Justitie (WODC) en van het Nationaal Programma ITeR. Het is een rechtsvergelijkend onderzoek ter ondersteuning van het Ministerie van Justitie bij het vervaardigen van de nota *Internationalisering en recht in de informatiemaatschappij*, die als vervolg op de nota *Wetgeving voor de elektronische snelweg* (hierna: nota WES) in het voorjaar van 2000 aan de Tweede Kamer wordt aangeboden. Het onderhavige onderzoek is een vervolg op de studie *Netiquette of Wetiquette*, die het Centrum voor Recht, Bestuur en Informatisering in 1997 schreef ter ondersteuning van de nota WES.

De doelstelling van deze studie is in vogelvlucht een overzicht te geven van de opvattingen van de buitenlandse overheden over de belangrijkste thema's op het gebied van ICT-recht in het licht van internationalisering en rechtsmacht. Vanwege de korte looptijd van het onderzoek – januari tot en met april 2000 – en het brede onderzoeksveld, hebben wij de studie in enkele opzichten beperkt.

In de eerste plaats hebben wij, in overleg met de opdrachtgever, het onderzoek beperkt tot de vier landen die voor Nederland het meest relevant zijn bij de ontwikkeling van een nationaal beleid dat aansluit op internationale standpunten: Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten. Om toch tegemoet te komen aan interessante ontwikkelingen op ICT-rechtsgebied in landen als Zweden, Canada, Singapore en Australië, die voor de ontwikkeling van een internationaal afgestemd ICT-rechtsbeleid evenzeer relevant kunnen zijn, hebben wij bij sommige onderwerpen aandacht besteed aan standpunten en ontwikkelingen in deze andere landen, met name waar deze afwijken van de gesignaleerde standpunten en ontwikkelingen in de vier onderzochte landen.

In de tweede plaats is de reikwijdte van het onderzoek beperkt qua onderwerpen. In overleg met de opdrachtgever hebben wij ervoor gekozen om de drie belangrijkste algemene thema's van de nota WES te onderzoeken, te weten zelfregulering, het adagium "online = offline" en handhaving. Deze algemene thema's werken door in alle onderwerpen van het ICT-recht waar beleid voor moet worden gemaakt. Om te kijken hoe deze thema's doorwerken in specifieke onderwerpen, hebben wij gekozen voor bestudering van vier "capita selecta" die de opdrachtgever het interessantst vond: samenwerking tussen strafrechtelijke handhavingsautoriteiten, dubbele strafbaarheid, totstandkoming van online overeenkomsten en civiele aansprakelijkheid van Internet-aanbieders.

In de derde plaats is het onderzoek beperkt in diepgang: het onderzoek heeft het karakter van een "quick scan". Wij hebben ons beperkt tot de standpunten van de overheden die in officiële beleidsdocumenten zijn te vinden en de belangrijkste wetgeving die op het terrein van ICT-recht bestaat of in voorbereiding is. Bij de landen met een federale structuur (VS, Duitsland) hebben wij ons beperkt tot de federale overheid.

Door de verleende opdracht ligt de nadruk in deze studie op de standpunten van *nationale* overheden over ICT-recht. Dit hangt samen met de wens van de opdrachtgever om de

belangrijkste nationale standpunten op diverse onderwerpen te leren kennen, zodat Nederlandse afgevaardigden in internationale onderhandelingen en besprekingen hun positiebepaling daarop kunnen afstemmen. Deze studie legt daarom de nadruk op de standpunten van de overheden van Duitsland, Frankrijk, het VK en de VS. In zekere zin is dat een vertekening van de werkelijkheid, omdat veel ICT-recht en -beleid worden voorbereid en afgestemd in internationale fora en door internationale organisaties. Daarom hebben we bij elk onderwerp in het begin aangegeven wat de belangrijkste ontwikkelingen zijn binnen internationale organisaties, hetgeen een kader geeft voor de standpunten van de nationale overheden die volgen.

Het onderzoek heeft plaatsgevonden door literatuurstudie en een internationale workshop. De literatuurstudie is gebaseerd op onderzoek van de officiële beleidsdocumenten, wetgeving en jurisprudentie, zoals die op de diverse weblocaties van de onderzochte overheden en instanties te vinden zijn, alsmede op artikelen en berichten in de literatuur (waaronder *Computer und Recht*, *The Computer Law & Security Report*, *Computer and Telecommunications Law Review* en *Electronic Commerce and Law Report*). Dit onderzoek is ondersteund door bijdragen van correspondenten uit Frankrijk en het Verenigd Koninkrijk, die een volledige vragenlijst hebben ingevuld over de onderzochte onderwerpen, en door correspondenten uit Duitsland en de VS, die op specifieke onderwerpen nadere informatie hebben gegeven.

De voorlopige resultaten van het onderzoek die medio maart beschikbaar waren, zijn getoetst op een internationale workshop die de onderzoekers op 29 maart 2000 in Amsterdam hebben gehouden. Aan deze workshop namen 21 deskundigen op het gebied van ICT-recht en -beleid deel. Tijdens de workshop zijn de drie algemene thema's en selecte onderwerpen uit het civielrecht en strafrecht besproken. De uitkomsten van de workshop zijn vervolgens verwerkt in deze studie. Waar relevant hebben wij ook in dit rapport de uitkomsten van de workshop expliciet als zodanig vermeld, aangezien de deskundigheid van de deelnemers het gebruik van de conclusies van de workshop als een zelfstandige onderzoeksbron rechtvaardigt. Het verslag en een lijst met de deelnemers van de workshop zijn opgenomen in bijlage IV.

Wij zijn terzijde gestaan door een begeleidingscommissie, die de onderzoeksresultaten tijdens twee vergaderingen heeft besproken en van kanttekeningen heeft voorzien. Wij danken de leden van de begeleidingscommissie voor hun bijdragen, die een waardevolle ondersteuning zijn geweest bij de vervaardiging van de eindrapportage.

Het onderzoek is uitgevoerd van 1 januari tot en met 30 april 2000. De rapportage is afgerond op 1 mei 2000.

Inhoudsopgave

1. Inleiding

1.1 De ontwikkeling van ICT-recht

In korte tijd heeft de elektronische snelweg de (Westerse) wereld veroverd. Waar begin jaren negentig van de vorige eeuw nog maar weinigen gehoord hadden van e-post of Internet, zijn deze technieken nog geen tien jaar later geïnstitutionaliseerd en alledaags geworden. De invloed hiervan op de maatschappij is nog moeilijk te overzien, maar het staat wel vast dat de wereld met een elektronische snelweg in diverse opzichten anders functioneert dan de wereld van tien jaar geleden. Dat heeft zijn weerslag op het recht.

Met de opkomst van informatie- en communicatietechnologie (ICT) en de elektronische snelweg is ook het ICT-recht gegroeid. Terwijl diverse deelterreinen van het recht al sinds de jaren zeventig van de vorige eeuw bezig zijn de ontwikkelingen in ICT bij te houden, is in de jaren negentig onderkend dat de opkomst van ICT en de elektronische snelweg ook een meer fundamentele invloed op het recht als geheel heeft. ICT beïnvloedt immers alle aspecten van het maatschappelijk leven, en daardoor snijdt het ICT-recht dwars door de traditionele rechtsgebieden heen. De vraag kwam dan ook op hoe het recht als geheel moest reageren op deze ontwikkelingen. Met de nota *Wetgeving voor de elektronische snelweg* (Nota WES) heeft het Nederlandse kabinet in 1998 geprobeerd om deze vraag te beantwoorden. Ook in andere landen is uitvoerig stilgestaan bij de problemen die ICT-ontwikkelingen het recht stellen.

Bij de beantwoording van ICT-rechtsvragen moet in acht worden genomen dat ICT een sterk internationaliserende werking heeft – de elektronische snelweg is bij uitstek een grensoverschrijdend verschijnsel. Dit leidt direct tot vragen over rechtsmacht: welk recht is van toepassing op handelingen die zich over meerdere rechtsgebieden tegelijk uitstrekken, zonder dat op voorhand duidelijk is op welk grondgebied de "Cyberspace-handeling" heeft plaatsgevonden? En hoe valt dat te rijmen met uiteenlopende nationale regelingen die verschillende maten van rechtsbescherming bieden? De aspecten van internationalisering en rechtsmacht zijn daarom inherent verbonden aan het ICT-recht, en dat hebben overheden die zich de taak stelden om ICT-recht te vormen zich ook altijd gerealiseerd.

Desondanks is het aspect van internationalisering en rechtsmacht bij de daadwerkelijke beantwoording van concrete ICT-rechtsvragen niet altijd in ogenschouw genomen. Vaak was het probleem in de nationale context van het nationale recht al moeilijk genoeg oplosbaar, zodat er weinig ruimte was voor gedachtevorming over de internationale dimensie van het probleem. Voor veel vraagstukken op ICT-rechtsgebied betekende dit dat tot nu toe de aandacht primair gericht is geweest op de nationale context.

Op langere termijn is dat geen werkbare situatie. ICT-recht dat primair vanuit de nationale context wordt gevormd, stuit in de internationale ICT-samenleving op problemen. Uiteenlopende nationale regelingen leiden tot verschillen in

rechtsbescherming en in verschillende voorwaarden voor elektronische handel, hetgeen haaks staat op de internationaal breed gedragen wens te komen tot een internationale markt voor elektronische handel. Het ICT-recht moet dus niet primair vanuit de nationale context vorm krijgen, maar vanuit de internationale context. Dat betekent niet dat ICT-recht alleen op internationaal niveau kan worden gevormd, maar veeleer dat overheden bij het maken van ICT-recht nadrukkelijk rekening moeten houden met de internationale context waarin het object van de regeling moet gedijen.

1.2 Doelstelling en opbouw

In deze studie bekijken wij hoe diverse overheden bij het nadenken over en het vormgeven van ICT-recht het perspectief van internationalisering en rechtsmacht betrekken. De doelstelling van deze studie is in vogelvlucht een overzicht te geven van de opvattingen van de overheden van Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten over de belangrijkste thema's op het gebied van ICT-recht in het licht van internationalisering en rechtsmacht.

Als kader voor de studie geven we in de rest van dit hoofdstuk de grote lijnen van het overheidsbeleid van de onderzochte landen op ICT-rechtsgebied weer, zoals dat in officiële beleidsdocumenten en wetgeving is vastgelegd.

In het eerste deel van deze studie geven wij vervolgens een overzicht van ideeën over drie alomvattende thema's die het ICT-recht in de breedte doorsnijden: de vraag of voor de elektronische snelweg dezelfde of juist andere regels moeten gelden als voor de 'traditionele' wereld (hoofdstuk 2), de vormgeving van die regels en de rol van zelfregulering daarbij (hoofdstuk 3) en de vraag hoe de handhaving van de regels kan worden gewaarborgd (hoofdstuk 4). Deze algemene thema's geven aan welke uitgangspunten of kaders overheden vaststellen of beogen voor ICT-recht in het algemeen.

In het tweede deel van deze studie volgen enkele 'capita selecta' van ICT-recht, verspreid over het strafrecht en het civielrecht: het vereiste van dubbele strafbaarheid (hoofdstuk 5) en de samenwerking tussen strafrechtelijke handhavingsautoriteiten (hoofdstuk 6), en vervolgens het vraagstuk van toepasselijk recht op online overeenkomsten (hoofdstuk 7) en de civielrechtelijke aansprakelijkheid van Internet-aanbieders (hoofdstuk 8). Deze specifieke onderwerpen geven aan hoe de beoogde algemene uitgangspunten en kaders in concreto uitwerken.

De studie wordt afgesloten met een samenvatting en conclusies (hoofdstuk 9).

1.3 Duitsland over ICT-recht en -beleid

In Duitsland werden de eerste stappen voor de ontwikkeling van wetgevingsbeleid inzake de elektronische snelweg in 1996 gezet met de publicatie van het rapport *Info 2000: Deutschland s Weg in die Informationsgesellschaft* (hierna: Info 2000-rapport).[1] De Duitse regering wees reeds in dit rapport op de noodzaak van een internationaal juridisch kader voor de problematiek. De Duitse regering zette vervolgens beleidsvoornemens uiteen rond multimedia in de beleidsnota *Multimedia möglich machen. Deutschland s Weg in die Wissensgesellschaft*[2] uit februari 1998 van het Bondsministerie voor Onderwijs, Wetenschap, Onderzoek en Technologie.

1 BMWi 1996.
2 BMBF 1999.

Een direct uitvloeisel van de in het Info 2000-rapport gelanceerde plannen was de Multimediawet, Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG)[3] van de federale overheid, die grotendeels op 1 augustus 1997 in werking trad. Deze wet regelt als kaderwet een aantal zaken, waaronder telediensten en de aansprakelijkheid van Internet-aanbieders (Teledienstegesetz, art. 1), de bescherming van persoonsgegevens bij telediensten (Teledienstedatenschutzgesetz, art. 2) en digitale handtekeningen (Gesetz zur digitalen Signatur, art. 3), en past ook bestaande wetgeving aan. Verder hebben de Länder een Mediendienste-Staatsvertrag (MDStV) afgesloten, in werking getreden op 1 augustus 1997, dat de (omroep-)mediadiensten regelt.

Zoals de Duitse regering al had aangekondigd, werd de IuKDG in 1999 geëvalueerd. Daarbij bleek dat er geen aanleiding bestond de IuKDG ingrijpend aan te passen. Op enkele aspecten na, was de Bondsregering tevreden over de uitwerking van het wetgevingsbeleid inzake de elektronische snelweg.

Medio 1999 werd de volgende stap genomen: het Actieprogramma *Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts*.[4] In dit programma spreekt de Bondsregering de ambitie uit in de komende jaren te komen tot één juridisch ordeningskader voor telecommunicatiemiddelen, media en telediensten. Diverse huidige wetten (naast de IuKDG, het Mediendienste-Staatsvertrag en het Telekommunikationsgesetz) dienen geheel dan wel deels in dit ordeningskader te worden opgenomen.

1.4 Frankrijk over ICT-recht en -beleid

Op 25 augustus 1997 kondigde premier Jospin een informatiemaatschappij-actieplan aan voor de Franse overheid,[5] dat vervolgens in januari 1998 werd gepubliceerd: het *Programme d Action Gouvernemental pour la Société de l Information* (PAGSI).[6] Het actieprogramma wil onder andere een doelmatige regeling en de ontwikkeling van een beschermend kader voor de informatiemaatschappij bevorderen. Een jaar later werd de voortgang van het actieprogramma besproken door het Comité Interministériel pour la Société de l'Information (CISI), waarbij op diverse terreinen standpunten werden ingenomen of aangescherpt.[7] Inmiddels had de Conseil d'Etat (de Raad van State) in juli 1998 een uitgebreid advies gepubliceerd over regelgeving voor elektronische snelwegen: *Internet et les résaux numériques*.[8] Het Ministerie van Economische Zaken heeft in het Lorentz-rapport van januari 1998,[9] het addendum daarop van maart 1998[10] en de evaluatie daarvan een jaar later[11] specifiek aandacht besteed aan de elektronische handel en voorstellen gedaan voor het juridische kader voor e-handel.

Na deze formuleringen van beleidsuitgangspunten en -voornemens, heeft de regering vervolgens in november 1999 een omvattend consultatiedocument uitgebracht, dat moet leiden tot een wetsvoorstel over de informatiemaatschappij: *Une société de l information pour tous. Adaptation du cadre législatif de la société de l information. Document d orientation soumis à consultation publique*.[12] Het wetsvoorstel zou drie pijlers moeten hebben: de verheldering van de rechten en plichten van eenieder, de

3 WWW <http://www.iid.de/rahmen/iukdgebt.html>.
4 Bundesregierung 1999.
5 Jospin 1997.
6 PAGSI 1998.
7 CISI 1999.
8 Conseil d'Etat 1998.
9 Lorentz 1998a.
10 Lorentz 1998b.
11 Lorentz 1999.
12 Strauss Kahn et al. 1999.

democratisering van de toegang tot de informatiemaatschappij, en de veiligheid en het vertrouwen in elektronische transacties. De regering beoogt het wetsvoorstel in 2000 aan het parlement voor te leggen; op 1 mei 2000 was dit nog niet beschikbaar.

Vermeldenswaard is dat de Franse regering een speciale weblocatie voor het informatiemaatschappij-actieplan heeft opgezet: <www.internet.gouv.fr>, waar een overzicht wordt gegeven van de diverse overheidsactiviteiten op dit terrein.

1.5 Het Verenigd Koninkrijk over ICT-recht en -beleid

De Britse regering publiceerde haar beleidsvoornemens voor de informatiemaatschappij en het Internet in 1998. Het beleidsdocument *Our Information Age. The Government s Vision* zet de ideeën uiteen van de regering over een gecoördineerde strategie voor het informatietijdperk, om onder andere de concurrentiekracht te verhogen en kwaliteit te waarborgen.[13] De Minister voor Wetenschap, energie en bedrijfsleven John Battle zette vervolgens nog eens de regeringsstrategie voor het Internet uiteen in een toespraak in het House of Commons op 18 maart 1998.[14] Hierin formuleerde hij vier principes voor de regulering van het Internet: wat offline geldt, moet ook online gelden, internationale samenwerking is noodzakelijk, bedrijven en consumenten moeten middelen hebben om zichzelf te beschermen, en dienstaanbieders moeten zelfreguleringsinitiatieven nemen om het recht te handhaven. Aansluitend heeft de regering haar beleid voor het informatietijdperk bijeengebracht en samengevat op een weblocatie: *The Government s policy for the information age*, <http://www.isi.gov.uk/isi/infosoc/govpolicy.htm>,[15] terwijl ook een E-Minister, Patricia Hewitt,[16] en een E-Envoy, Alex Allan,[17] zijn aangesteld.

Naast het overkoepelende beleid voor de informatiemaatschappij, heeft de Britse overheid vooral de nadruk gelegd op elektronische handel, met name in het rapport *E-Commerce@its.best.uk*, dat een strategie geeft om "het Verenigd Koninkrijk de beste omgeving ter wereld voor e-handel te maken".[18] Dit leidde eind 1999 tot het indienen van een wetsvoorstel met een juridisch kader voor elektronische handel, de *Electronic Communications Bill*. Het House of Commons nam het wetsvoorstel in geamendeerde vorm aan, waarna het op 26 januari 2000 bij het House of Commons werd ingediend.[19]

Vermeldenswaard is overigens dat al in juli 1996, ruim voor de regering haar beleid formuleerde, het Britse House of Lords een actie-agenda voor de informatiemaatschappij had opgesteld, waarin diverse beleidsvoorstellen werden gedaan.[20] Het Britse House of Commons ging in 1999 nader in op het beleid voor de informatiemaatschappij.[21]

13 Blair 1998.
14 Battle 1998.
15 ISI 1999.
16 Zie <http://www.e-envoy.gov.uk/2000/strategy/workstreams/programme_management/e-minister.htm>.
17 Zie <http://www.e-envoy.gov.uk>.
18 Cabinet Office 1999.
19 Zie <http://www.parliament.the-stationery-office.co.uk/pa/ld199900/ldbills/024/2000024.htm>.
20 House of Lords 1996.
21 House of Commons 1999.

1.6 De Verenigde Staten over ICT-recht en -beleid

De overheid van de Verenigde Staten heeft geen beleidsdocumenten over de elektronische snelweg of het Internet gepubliceerd, maar heeft zich geconcentreerd op beleid voor de elektronische handel. Op 1 juli 1997 publiceerden president Clinton en vice-president Gore de beleidsnota *A Framework For Global Electronic Commerce*,[22] tegelijk met een *Presidential Directive*.[23] Zowel in deze nota als in het eveneens in 1997 verschenen FCC-rapport *Digital Tornado: The Internet and Telecommunications Policy*[24] opteert de Amerikaanse regering voor een niet-regulatieve, op de markt georiënteerde benadering van de elektronisch handel, die het ontstaan van een transparante en voorspelbare juridische omgeving bevordert. Belangrijke uitgangspunten hierbij zijn de voortrekkersrol voor de private sector en een "minimalistische, consistente, voorspelbare en eenvoudige juridische omgeving voor de elektronische handel".

Wat betreft het thema internationalisering en rechtsmacht kan worden vermeld dat de beleidsnota aangaf dat de elektronische handel op wereldwijde basis bevorderd moet worden, waarbij het juridische raamwerk dient te bestaan uit beginselen die internationaal voorspelbare resultaten opleveren, ongeacht de jurisdictie waartoe partijen behoren.

In 1998 publiceerden diverse individuele overheidsorganisaties rapporten en plannen over kwesties op het terrein van ICT-recht. Zo bracht het Department of Commerce het rapport *The Emerging Digital Economy* uit,[25] en publiceerde de National Science Foundation het programma *Digital Government*.[26]

Op 29 november 1999, ruim twee jaar na de publicatie van het *Framework*, gaf president Clinton opdracht tot het instellen van een Electronic Commerce Advisory Group, een sub-werkgroep van de US Government Working Group on Electronic Commerce. Deze adviesgroep heeft tot taak de juridische barrières te identificeren die de verdere groei van de elektronische handel in de weg staan. Clinton wees daarbij nadrukkelijk op de noodzaak te komen tot een uniforme aanpak van wetgevende maatregelen. Naast de opdracht aan de adviesgroep "to discuss ways to ensure that public interest protections for online transactions will be equivalent to those now provided for offline transactions", gaf Clinton de adviesgroep nog drie uitgangspunten mee die centraal dienen te staan bij het doen van aanbevelingen: "technological neutrality, minimize legal and regulatory barriers to electronic commerce; and take into account cross-border transactions that are now likely to occur electronically."[27]

Alhoewel het ICT-recht en -beleid in de VS voor een belangrijk deel wordt overgelaten aan de markt, wordt het regulerend kader toch ook bepaald door enkele belangrijke wetten, zoals de Telecommunications Act 1996 en niet in de laatste plaats ook door enkele Amendments uit de Grondwet.

---

22 White House 1997.
23 Clinton 1997.
24 FCC 1997.
25 Department of Commerce 1998.
26 Zie <http://www.nsf.gov/pubs/1998/nsf98121/nsf98121.htm>.
27 White House 1999.

1.7 Overzicht van overheden over ICT-recht en -beleid

Uit de beleidsdocumenten die hierboven zijn aangegeven, valt voor elk land een globaal beeld te vormen van de overkoepelende visie op ICT-recht en -beleid, alsmede de doelstellingen en de strategie van elke overheid. In vrijwel alle documenten ligt de nadruk op elektronische handel, waarvoor een juridisch raamwerk moet worden gemaakt. In bijlage I geven we een indicatie van deze aspecten voor elk land.

Deel I – Algemene thema's

2. De relatie tussen offline en online

2.1 Inleiding

De Nederlandse regering heeft bij meerdere gelegenheden laten weten dat in de discussie over regulering van ontwikkelingen als elektronische handel, Internet en meer in het algemeen de elektronische snelweg, de rode draad dient te zijn: "wat offline geldt, moet in principe ook online gelden". In de Nota WES stelt het kabinet het in relatie tot internationalisering en rechtsmacht als volgt: "In de eerste plaats kiest het kabinet als uitgangspunt dat de normen die gelden voor de elektronische snelweg hetzelfde dienen te zijn als de normen in de fysieke wereld."[28] In bepaalde situaties zal aan dit uitgangspunt echter geen invulling gegeven kunnen worden. Zo zal in die situaties dat de traditionele wettelijke bepalingen voor de fysieke wereld tot problemen leiden bij toepassing in een elektronische omgeving bezien moeten worden of er andere regels dienen te gelden. Hiernaast laten bestaande en toekomstige Europese en internationale afspraken soms geen ruimte voor het doorzetten van het adagium.[29] Aldus zal derhalve de wens te komen tot een internationale aanpak van bepaalde ICT-gerelateerde problemen tot resultaat hebben dat voor de offline en de online andere regels gelden.[30]

2.2 Internationale organisaties

Wat betreft de relatie tussen online en offline kan worden vastgesteld dat voorzover de diverse internationale organisaties en fora aandacht aan dit thema besteden, ze in zijn algemeenheid het standpunt huldigen dat de online wereld geen op zichzelf staande nieuwe wereld is. Aldus gelden in principe voor de online wereld dezelfde normen als voor de offline wereld. Deze constatering wordt bevestigd door de diverse beleidsplannen op een internationaal niveau: bij het formuleren wordt uitgegaan van de regels die gelden voor de offline wereld.[31] Uitsluitend ten behoeve van bepaalde belangen (zoals de rechtszekerheid) worden eventueel nadere regels gesteld.

Toch laat de praktijk zien dat deze benadering op een internationaal niveau wordt losgelaten als het aankomt op het vormgeven van bepaalde beleidsprioriteiten. Een duidelijk voorbeeld is de Europese richtlijn elektronische handel, waarin ter bevordering van de gemeenschappelijke markt voor elektronische handel (eventueel zelfs ten koste van de handel in de offline wereld) specifieke regels voor de online wereld worden gesteld.

---

28 Nota WES, p. 114.

29 Zie bijvoorbeeld het antwoord van de Minister van Justitie op vragen van de vaste commissie voor Justitie in: TK 1999-2000, 26538, nr. 2, p. 5.

30 Nota WES, p. 114.

31 Zie ook Den Haan 1998, p. 30.

2.3 Duitsland

Het voornoemde standpunt van de Nederlandse regering is nergens als zodanig terug te vinden in de Duitse beleidsdocumenten. Toch zou men uit de voorgestelde aanpak in de diverse beleidsdocumenten kunnen afleiden dat het adagium in Duitsland in het algemeen wel steun vindt. Een blik op de IuKDG leert echter dat wanneer het op de regulering van concrete onderwerpen aankomt, er in de online wereld toch andere regels gelden dan de traditionele wereld. Een voorbeeld hiervan is de regeling van §5 Teledienstegesetz, waar bepaalde Internet-aanbieders geprivilegieerd worden boven traditionele pers-tussenpersonen.

2.4 Frankrijk

Alhoewel de Franse regering nergens als zodanig het uitgangspunt "wat offline geldt, dient ook online te gelden" formuleert, is het standpunt wel degelijk uit de diverse opmerkingen in de beleidsdocumenten af te leiden. Zo merkt de Conseil d'Etat in het van 2 juli 1998 daterende rapport *Internet et les réseaux numériques* het navolgende op: "Tout d'abord, contrairement à ce que l'on entend parfois, l'ensemble de la legislation existante s'applique aux acteurs d'Internet", waar men aan toevoegt dat dit met name geldt voor consumentenbescherming en aspecten van het publiek belang. Kortom: "Il n'existe pas et il n'est nul besoin d'un droit spécifique de l'Internet et des réseaux."

Toch onderkent de regering ook dat ten behoeve van de bescherming van bepaalde belangen – concreet wordt gewezen op consumentenbelangen en de aanpak van illegale en schadelijke inhoud – wellicht specifieke regels zullen moeten worden gëntroduceerd.[32]

2.5 Verenigd Koninkrijk

De Britse regering heeft het standpunt "wat offline geldt, moet ook online gelden" expliciet verwoord in *Her Majesty s Government Strategy for the Internet* van 18 maart 1998. Het uitgangspunt is aangemerkt als het eerste van de vier uitgangspunten in het beleid van het Verenigd Koninkrijk: "First, existing law should apply on-line as it does off-line. With very few exceptions where this is not possible, this is already the case in the UK."[33]

Ook wordt gewezen op het belang van dit standpunt bij grensoverschrijdende aspecten: "Neutrality between trade carried out on-line and off-line should be the key principle underpinning any future consideration of the relationship between electronic commerce and international trade".[34]

Het algemene standpunt wordt in diverse documenten nader toegespitst op concrete onderwerpen. Zo gaf de Engelse Data Registrar aan: "although the application of the technologies involved in e-commerce are new the data protection issues which arise are not. The provisions of the Data Protection Acts 1984 and 1998 apply to the processing of personal data on-line as much as off-line".[35]

Toch blijkt ook hier dat het uitgangspunt niet altijd gehandhaafd kan blijven. Zo toont de Electronic Communications Bill uit 1999, die de Europese richtlijnen op de terreinen van elektronische handtekeningen, verkoop-op-afstand en andere e-handelaspecten moet implementeren, dat er wel degelijk verschillen ontstaan in de regels in de online

32 Zie onder meer PAGSI 1998, p. 58, en Strauss Kahn e.a. 1999, p. 31.
33 Battle 1998.
34 House of Commons 1999, p. 7-8.
35 Geciteerd in House of Commons 1999, p. 9.

wereld en de offline wereld. Ook de visie die momenteel in het Verenigd Koninkrijk wordt ontwikkeld op het thema convergentie laat zien dat er onderwerpen zijn die in de online wereld een andere benadering vereisen.[36]

Tijdens de internationale workshop werd door een deskundige uit het Verenigd Koninkrijk opgemerkt dat het hanteren van de 'online = offline'-benadering een volstrekte illusie is. Propageren van dit adagium is niet meer dan vasthouden aan een romantisch en verouderd concept. In plaats hiervan zal bezien moeten worden *waarom* er bepaalde regels in de offline wereld zijn en *waarom* deze regels in de online wereld gehandhaafd zouden moeten blijven. Daarbij zal de wetgever uitdrukkelijk aandacht moeten hebben voor de achterliggende doelstellingen van de betreffende regels. Indien de online wereld specifieke verschillen met de offline wereld introduceert, zal bezien moeten worden wat het effect van deze verschillen is op de bestaande regels, daarbij de ratio van deze regels in overweging nemende. In plaats van de regels van de fysieke wereld automatisch te transponeren naar de online wereld, moet de wetgever creatief op zoek gaan naar oplossingen voor de specifieke problemen van de online wereld.

Tevens werd door de deskundigen uit het Verenigd Koninkrijk tijdens de internationale workshop opgemerkt dat de benadering 'offline = online' ook de andere kant op kan werken: "wat online geldt, dient ook offline te gelden". Kortom, de wetgever moet oog hebben voor de interactie tussen de regels uit de twee werelden en niet uitsluitend redeneren vanuit de regels van de offline wereld.

2.6 Verenigde Staten

President Clinton gaf op 29 november 1999 opdracht tot het instellen van een Electronic Commerce Advisory Group, als sub-werkgroep van de US Government Working Group on Electronic Commerce. Deze adviesgroep kreeg tot taak de juridische barrières te identificeren die de verdere groei van de elektronische handel in de weg staan. Van belang voor het thema "wat offline geldt, dient ook online te gelden" is de boodschap die Clinton aan de werkgroep meegaf: de aanbevelingen van de adviesgroep moeten "discuss ways to ensure that public interest protections for online transactions will be equivalent to those now provided for offline transactions". Concreet stelt Clinton dat "it is critical that consumers and the public at large be assured of a level of protection in electronic commerce equivalent to that which they now enjoy in more traditional forms of commerce".[37]

In het rapport *The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet* van maart 2000 merkt de President's Working Group on Unlawful Conduct on the Internet op dat "substantive regulation of unlawful conduct (…) should as a rule apply in the same way to conduct in the cyberworld as it does to conduct in the physical world." Vervolgens stelt de werkgroep dat de analyse in het rapport laat zien dat "existing substantive law is generally sufficient to cover unlawful conduct involving the use of the Internet".

Toch wordt ook onderkend dat dit uitgangspunt niet altijd doorgetrokken kan worden: "At the same time, we must recognize that different media may require different approaches and that public interest protections designed for the physical world may not fit in the electronic commerce arena. We should attempt to develop an equivalent level of protection, recognizing that different means may be necessary to accomplish that goal."

Dat de Verenigde Staten onderkennen dat het adagium "wat offline geldt, dient ook online te gelden" niet altijd het uitgangspunt kan zijn, blijkt opnieuw uit een uitspraak van Department of Commerce Secretary W.M. Daley op 1 februari 2000: "Some laws

36 Zie <http://www.culture.gov.uk/CONREP.htm>.

37 White House 1999.

and regulations designed for the 'physical world' may not always work in cyberspace." Daley wees erop dat "many current laws pre-date the expansion of electronic commerce and some licensing requirements or technical standards may inadvertently serve to prevent online transactions, while others may continue to make sense."[38]

Ten slotte werd tijdens de internationale workshop door een deskundige uit de Verenigde Staten opgemerkt dat bij de discussie over de offline/online-benadering het aspect van de handhaving van cruciaal belang is. Bij het denken over de rol van het adagium 'online = offline' zal nadrukkelijk aandacht besteed moeten worden aan de gevolgen daarvan voor de rechtshandhaving.

2.7 Vergelijking en conclusie

Uit de bovenstaande analyse blijkt dat de regeringen van Frankrijk en het Verenigd Koninkrijk het adagium "wat offline geldt, dient ook online te gelden" impliciet (Frankrijk) of expliciet (VK)[39] als uitgangspunt hebben geformuleerd. Toch laten wetgevingsinitiatieven op concrete onderwerpen zien dat het uitgangspunt niet altijd wordt vastgehouden.

In de Duitse documenten is het standpunt niet als zodanig terug te vinden, wel blijkt het er impliciet uit. Een blik op de IuKDG leert echter ook dat wanneer het op de regulering van concrete onderwerpen aankomt, er in de online wereld toch andere regels kunnen gelden dan de traditionele wereld.

Recente ontwikkelingen in de Verenigde Staten ten slotte laten zien dat alhoewel men belang hecht aan een gelijke uitgangspunten voor de online en de offline wereld, men tevens uitdrukkelijk vaststelt dat het uitgangspunt niet altijd doorgetrokken zal kunnen worden. Vermeld moet hierbij worden dat wanneer de Amerikaanse regering spreekt over de relatie tussen de offline en de online wereld, men niet zozeer stelt dat de concrete regels hetzelfde dienen te zijn, maar dat het beschermingsniveau in beide werelden gelijk moet zijn.

In geen van de onderzochte landen is een expliciet standpunt ingenomen over een algemene Lex Internet, een overkoepelende wet die alle aspecten van het Internet zou moeten regelen. De Nederlandse regering noemde in de Nota WES een Lex Internet nu niet opportuun, maar op termijn wel een interessante optie.[40]

Concluderend kunnen we stellen dat het adagium "wat offline geldt, dient ook online te gelden" tot voor kort in de diverse landen als algemeen uitgangspunt navolging kreeg. Meer recent is echter gebleken dat het in toenemende mate problematisch wordt om deze benadering consequent door te voeren bij de aanpak van de diverse specifieke problemen. Het adagium blijkt bij de uitwerking van concrete onderwerpen het onderspit te moeten delven, omdat er – gegeven bepaalde belangen (zoals consumentenbescherming, rechtszekerheid, bevordering van de elektronische handel) – toch specifieke regels voor de online wereld worden gä ntroduceerd. Deze tendens is ook op een internationaal niveau (in ieder geval de Europese Unie) waarneembaar.

---

38 Geciteerd in *Electronic Commerce & Law Report*, 9 februari 2000, p. 138-139.

39 Ook Australië heeft het standpunt "wat offline geldt, dient ook online te gelden" expliciet verwoord in beleidsdocumenten. Als een van de principes van de overheidsbeleid wordt genoemd: "provide for functional equivalence, i.e. online transactions will be treated similarly to offline transactions". Zie <http:// www.noie.gov.au/legreg/body_index.htm>. Evenzo, aldus een speech van de verantwoordelijke minister: "What is illegal offline should be illegal online". Zie <http:// www.noie.gov.au/legreg.htm> onder *speeches*.

40 Nota WES, p. 119.

Tijdens de internationale workshop werd bevestigd dat het adagium in de begintijd van ICT-regulering (midden jaren negentig) zijn waarde kon bewijzen omdat daarmee kon worden vastgesteld dat Internet geen rechtsvacuüm was, maar dat het beginsel inmiddels niet meer is dan een romantisch en achterhaald concept. De complexiteit van de materie bewijst dat de problemen in de online wereld verschillen van die van de offline wereld. Aldus is het onverstandig om als vertrekpunt bij het denken over regulering vast te houden aan de concrete regels van de offline wereld. De benadering zal niet zozeer moeten zijn dat men de concrete regels van de online wereld in principe gelijkstelt aan die van de offline wereld, maar dat het beschermingsniveau in beide werelden gelijk moet zijn. Aldus zal de overheid veel meer aandacht moeten hebben voor de *belangen en doelstellingen* die aan de regels van de offline respectievelijk online wereld ten grondslag (moeten) liggen. De vraag die men zich dient te stellen is *waarom* er bepaalde regels in de offline wereld zijn en *waarom* deze regels in de online wereld gehandhaafd zouden moeten blijven. Indien de online wereld specifieke verschillen met de offline wereld introduceert, zal bezien moeten worden wat het effect van deze verschillen is op de bestaande regels, daarbij de ratio van deze regels in overweging nemende. In plaats van de regels van de fysieke wereld automatisch te transponeren naar de online wereld, moet de wetgever creatief zijn in het vinden van oplossingen voor de specifieke problemen van de online wereld.

Een ander punt dat naar voren komt is het feit dat de benadering 'offline = online' ook de andere kant op kan werken: "wat online geldt, dient ook offline te gelden". Kortom, de wetgever moet oog hebben voor de interactie tussen de regels uit de twee werelden en niet uitsluitend redeneren vanuit de regels van de offline wereld.

Ook moet worden vastgesteld dat bij de discussie over de offline/online-benadering het aspect van de handhaving van cruciaal belang is. De effectiviteit van de keuze voor een bepaald beleid staat of valt met de consequenties voor de handhaving van de gestelde regels. Bij het denken over de rol van het adagium 'offline = online' zal daarom nadrukkelijk aandacht besteed moeten worden aan de gevolgen voor de handhaving.

3. Zelfregulering

3.1 Inleiding

Zelfregulering is een centraal thema in de diverse nationale en internationale beleidsdocumenten. Zoals bekend toont de Nederlandse regering zich in de Nota WES een sterk voorstander van de inzet van zelfreguleringmechanismen bij het oplossen van de juridische onzekerheid over grensoverschrijdende consequenties van elektronische communicatie. Juist door op het instrument van de zelfregulering in te zetten, hoopt de overheid voldoende flexibiliteit te bieden in een tijd waarin technologische en maatschappelijke turbulentie de overhand hebben. Bijkomend voordeel is dat zelfregulering in principe niet aan landsgrenzen is gebonden, hetgeen eveneens een belangrijk voordeel is gegeven het grenzeloze karakter van het Internet. Overigens blijft naar de visie van de Nederlandse regering het instrument van overheidsregulering het uitgangspunt indien fundamentele normen en waarden van de rechtsstaat in het geding zijn.[41] Het kabinet noemt in dit verband de bescherming van klassieke grondrechten van burgers, de preventie en opsporing van inbreuken op de rechtsorde en de staatsveiligheid. In latere documenten is bijvoorbeeld ook het belang van consumentenbescherming in relatie tot veiligheid en betrouwbaarheid (bijvoorbeeld bij elektronisch betalen), privacy en toepasselijk recht genoemd.[42]

In de Nota WES wordt wel een taak voor de overheid toegedacht bij het toezicht op de randvoorwaarden die voor zelfregulering gelden. Deze randvoorwaarden zijn: doelgroepen dienen voldoende georganiseerd te zijn, gelijkwaardige behartiging van maatschappelijke belangen, voldoende binding van alle partijen, en de handhaving van de afspraken moet voldoende verzekerd zijn. De taak van de overheid kan vorm krijgen door:[43]

- het behartigen van onvoldoende vertegenwoordigde – kwetsbare – belangen;
- het opstellen ondersteunende wetgeving;
- het dreigen met wetgeving;
- het houden van toezicht;
- het meewerken aan handhaving (zoals via meldpunten).

Wanneer we het hebben over de specifieke rol van de overheid bij zelfregulering, kunnen we meerdere arrangementen onderscheiden. In de literatuur wordt gewezen op pure zelfregulering (waarbij de overheid geen sturende of initiërende rol heeft en alle initiatief bij de marktpartijen ligt), wettelijk geconditioneerde zelfregulering (waarbij de overheid dwingend bepaalde wettelijke randvoorwaarden stelt) en co-regulering (waarbij de overheid en de private sector als het ware hun krachten bundelen om te komen tot een beleid). Uit de navolgende analyse zal blijken dat het laatstgenoemde arrangement sterk

41 Nota WES, p. 180-181.
42 TK 1999-2000, 21501-15 en 23162, nr. 45, p. 3.
43 Nota WES, p. 181.

aan populariteit wint bij de regulering van ICT-problemen.[44] Daarbij zal overigens ook blijken dat er geen eenduidige opvatting bestaat over de vraag waar het concept van 'co-regulering' nu precies voor staat.

Gegeven de inzet van de Nederlandse regering op zelfregulering bij het oplossen van problemen die samenhangen met grensoverschrijdende elektronische communicatie, ligt de vraag voor in hoeverre deze visie aansluit bij het beleid van de relevante internationale organisaties en de in het kader van deze studie onderzochte landen. We bespreken in de navolgende paragrafen de in de diverse beleidsdocumenten verkondigde opvattingen, waarbij we overigens niet alleen stilstaan bij de visie op zelfregulering als zodanig, maar tevens de domeinen en onderwerpen aangeven waarvan wordt gesteld dat deze wel of niet dan wel deels aan zelfregulering kunnen worden overgelaten.

3.2 Internationale organisaties

Het algemene standpunt van de diverse internationale organisaties en fora (EU, Raad van Europa en OESO) over zelfregulering is positief. Daarbij valt wel op dat waar deze organisaties zich in het verleden een voorstander toonden van pure zelfregulering, men meer recentelijk een beleid uitdraagt waarbij co-regulering het uitgangspunt vormt. Zo toonde de OESO zich tijdens een conferentie te Parijs, in oktober 1999, een voorstander van een dergelijke vorm van regulering, waarbij men nadrukkelijk aangaf dat regulering een gezamenlijk optrekken van overheid en private partijen moet zijn.[45] Met name vanuit het belang van onder meer de rechtszekerheid en het beschermen van kwetsbare belangen (bijvoorbeeld van consumenten) moet zelfregulering aangevuld worden met overheidsregulering.

Wat betreft de rol van zelfregulering als middel om rechtsmachtproblemen aan te pakken valt geen standpuntbepaling uit de belangrijkste documenten af te leiden. In de documenten worden ook geen opmerkingen gemaakt over de mogelijke negatieve effecten van zelfregulering voor de internationale handel. Immers, zelfregulering kan het gevaar in zich hebben dat (onbedoeld) handelsbarrières worden opgeroepen. Te denken valt bijvoorbeeld aan de voorwaarden die in de diverse landen voor het voeren van een keurmerk voor veilige elektronische handel worden gesteld. In ene land kan daarmee aan bedrijven een hoger niveau van consumentenbescherming worden opgelegd dan in het andere land.

Overigens stellen we ook vast dat sommige organisaties bij specifieke onderwerpen wel voor overheidsinterventie pleiten. Waar het gaat om fundamentele beginselen van de rechtstaat (zoals privacybescherming) is pure zelfregulering en zelfs co-regulering geen geschikt beleidsinstrument. Een duidelijk voorbeeld hiervan is het standpunt van de Raad van Europa inzake de aanpak van delicten begaan met behulp van ICT (ontwerpverdrag *Crime in Cyberspace*).[46]

3.3 Duitsland

De rode draad door de Duitse aanpak is het motto "deregulering heeft voorrang boven regulering": "Dem deutschen Regelungsrahmen liegt der Gedanke zugrunde, daß der privaten Initiative grundsätzlich Vorrang vor hoheitlichen bzw. administrativen

44 Waarbij we opmerken dat, alhoewel deze variant van co-regulering pas recentelijk in de diverse beleidsdocumenten inzake ICT-recht opduikt, hij al langer wordt gepropageerd op andere beleidsterreinen, zoals het milieurecht. Vgl. de bijdragen in Eijlander e.a. 1993 en zie Prins & Van Kralingen 1997, die spreken over 'coproductie'.

45 OECD 1999, p. 11.

46 Waarvan op 27 april 2000 een ontwerp voor discussie werd gepubliceerd, Council of Europe 2000.

Maßsnahmen einzuräumen ist, um eine marktwirtschaftliche Entwicklung der Informationsgesellschaft zu gewährleisten."[47] Vanuit dit vertrekpunt beperkt de IuKDG zich tot het noemen van onderwerpen waarvan duidelijk is dat ze op zeer korte termijn nadere regulering behoeven om te komen tot een adequaat juridisch raamwerk voor de ontwikkeling van de informatiemaatschappij. Op deze wijze beoogt de IuKDG twee belangen veilig te stellen: a) rechtszekerheid en b) de bescherming van publieke belangen, zoals de bescherming van consumenten. Bij dit alles acht men het van groot belang dat het juridisch raamwerk technologische ontwikkelingen stimuleert en niet afremt.

Zoals de Duitse regering al had aangekondigd, werd de IuKDG in 1999 geëvalueerd. De markt werd hier nauw bij betrokken. Uit de evaluatie kwam naar voren dat er geen aanleiding bestond de IuKDG ingrijpend aan te passen. Op enkele losse deelgebieden na, waaronder de bescherming van consumenten en minderjarigen, bestaat er geen behoefte aan een aanpassing van het juridisch raamwerk. Wel blijkt het noodzakelijk de diverse regelingen op het terrein van de privacybescherming beter op elkaar af te stemmen, zodat het toepasselijke regime transparanter en gestroomlijnder is. Overigens stelt men wel vast dat de IuKDG alsmede de onderliggende regelingen mogelijk aangepast moeten worden ten gevolge van Europese regelgeving. In ieder geval kon worden vastgesteld dat het voornoemde motto van de Duitse aanpak niet behoeft te worden verlaten. Al met al kon constateerde Minister Müller: "Das Multimediagesetz hat eine wichtige Grundlage für die Entwicklung von E-Commerce in Deutschland gelegt."[48]

De voornoemde resultaten van de evaluatie zijn meegenomen in het Actieprogramma van de Bondsregering getiteld *Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts.*[49] De Duitse regering spreekt de ambitie uit te komen tot een juridisch ordeningskader voor telecommunicatiemiddelen, media en telediensten. Diverse huidige wetten (naast de IuKDG het Mediendienste-Staatsvertrag en het Telekommunikationsgesetz) dienen geheel of deels in dit ordeningskader te worden opgenomen.

Tevens geeft de regering aan dat ze het van groot belang acht bij het wetgevingsbeleid aandacht te hebben voor de belangen van consumenten en minderjarigen. Ook het recht op informationele zelfbeschikking staat hoog in het vaandel. Vanuit dit perspectief wordt in het Actieprogramma wetgeving aangekondigd op het terrein van consumentenbescherming (waarbij de Europese Richtlijn Verkoop-op-afstand centraal staat) en privacybescherming (er zal een nieuw wetgevingsconcept worden ontwikkeld, waarbij de huidige regels van het Teledienstedatenschutzgesetz worden gä ncorporeerd in het Bundesdatenschutzgesetz). Hiernaast wordt de campagne *Sicherheit in der Informationsgesellschaft*[50] gä ntensiveerd om het vertrouwen van burgers in het Internet te bevorderen. Ten slotte geeft de Duitse regering aan zich opnieuw actief op te stellen in de diverse internationale gremia, waarbij Internetbelasting en consumentenbescherming belangrijke aandachtspunten zijn.

Opvallend is dat het algemene beleidsuitgangspunt van zelfregulering nauwelijks als zodanig in het Actieprogramma is terug te vinden, maar dat de diverse actiepunten die worden aangekondigd in grote mate het belang van zelfregulering en eigen verantwoordelijkheid van de marktpartijen uitdragen. Men kan stellen dat het Actieprogramma duidelijk laat zien hoe het algemene beleidspunt van zelfregulering kan uitwerken in concrete wetgevingsvoorstellen. Als voorbeeld kan worden gewezen op de op het terrein van de privacybescherming aangekondigde actiepunten. Allereerst zal het

---

47 Stellungnahme der Bundesrepublik Deutschland zum Grunbuch der EU-Kommission "Konvergenz der Branchen Telekommunikation Medien und Informationstechnologie und ihre ordnungspolitischen Auswirkungen"; zie ook het rapport *Regulierung und Selbstregulierung* van 26 maart 1996 opgesteld door de projectgroep Rechtsprobleme des Internet.

48 BMWi 1999.

49 Bundesregierung 1999.

50 Zie <http:// www.sicherheit-im-internet.de>.

momenteel zeer complexe systeem van verschillende wettelijke regimes worden afgeslankt en vereenvoudigd. Tevens krijgt de eigen verantwoordelijkheid van de verwerkers van persoonsgegevens vorm via een vrijwillige – maar wettelijk verankerde – privacy-audit.

Een recent rapport waarin uitvoerig wordt ingegaan op de verhouding tussen zelfregulering en overheidsregulering op het terrein van schadelijke en illegale inhoud, is het rapport van de Bertelsmann-Stiftung van september 1999.[51] Van belang hier zijn de volgende opmerkingen in het rapport:

- "Providers party to an enforceable and broadly representative self-regulatory regime, recognized by public authorities, should not be liable for third party content when complying with the requirements of that regime and the decisions of the relevant selfregulatory body."
- "Laws should recognize (self-)rating and filtering mechanisms as well as age verification systems to exclude responsibility of providers for content harmful for children."
- "It is essential to have adequate legislative powers with respect to computer-based investigations, in particular, adequate powers for search and seizure. It would be helpful to make available a preservation order, which could 'freeze' evidence in a fast procedure and thus leave the decision about its delivery to a court judgement. In addition, legislation should be clearer on the obligations of Internet providers with respect to collection, storage and transfer to law enforcement of data relevant to investigations."

Uit het bovenstaande blijkt duidelijk dat men van de overheid verwacht dat ze de zelfregulerende aanbieders een bepaalde bescherming biedt. Op deze stellingname is inmiddels in de literatuur kritiek geuit omdat het de aanbieders veel macht tot controle in handen zou geven.

Ten slotte noemen we de in Duitsland opererende rechtsgeldige vereniging genaamd 'Freiwillige Selbstkontrolle Multimedia-Dienstenanbieter'. Hiernaast zijn Duitse bedrijven aangesloten bij de Internet Content Rating Association (ICRA).[52]

3.4 Frankrijk

De Franse regering onderkent in het PAGSI-rapport van januari 1998 dat de ontwikkeling van Internet en elektronisch handel de traditionele vormen van overheidssturing ter discussie stelt. Dit betekent echter niet dat we als overheid stil moeten zitten, aldus het rapport. Het uitgangspunt voor het Franse overheidsbeleid inzake ICT-regulering dient het onderscheid te zijn tussen enerzijds terreinen waar overheidsbemoeienis noodzakelijk is, omdat wettelijke regelingen aangepast dienen te worden ter facilitering van elektronische handel, en anderzijds terreinen waarop de overheid uitsluitend een voorbeeld dient te stellen, bijvoorbeeld door het stimuleren van ontwikkelingen. Toegespitst op regulering stelt men dat de overheid tot taak heeft:

- de noodzakelijke randvoorwaarden te stellen voor het bevorderen van het vertrouwen tussen dienstverleners en consumenten met betrekking tot elektronische handel;
- barrières te verwijderen die voortvloeien uit toepasselijke wetgeving en gewoonten omdat deze niet zijn toegesneden op de elektronische handel;
- toe te zien op de naleving van de diverse wettelijke vereisten.

51 Bertelsmann 1999, p. 46.

52 Zie <http://www.icra.org/pl.htm>.

Vanuit deze drie taken stelde de regering zich in 1998 ten doel in ieder geval op de volgende terreinen het vertrouwen van consumenten en de markt te bevorderen door bepaalde voorzieningen:

- bewijs, in het bijzonder elektronische handtekeningen;
- encryptie en betrouwbaarheid van berichtenverkeer;
- bescherming van persoonsgegevens;
- betalingssystemen die aansluiten bij Europese en internationale standaarden;
- toepasselijk recht, in het bijzonder in relatie tot consumentenaangelegenheden.

Wat betreft de rol van zelfregulering in de bovenstaande plannen merken zowel de Franse regering in het Actieprogramma als de Conseil d'Etat in het advies *Internet et les réseaux numériques*[53] op dat deze vorm van sturing in beeld dient te komen in al die situaties waarin het huidige wettelijke regime niet voorziet in een oplossing voor bepaald gedrag. Kort gezegd stelt men zich in Frankrijk op het standpunt dat het bestaande wetgevingsregime op het Internet en elektronische handel van toepassing is. Aan zelfregulering wordt een aanvullende rol toegekend. In dit verband wordt de ontwikkeling van de zogenaamde Netiquette[54] warm onthaald. Ook andere vormen van zelfregulering die op een realistische en effectieve wijze bijdragen aan de regulering van het Internet kunnen op de steun van de Franse regering rekenen, aldus het Actieplan.

Desalniettemin is de rol van zelfregulering een aanvullende en gebonden aan randvoorwaarden. Een belangrijke reden voor het stellen van randvoorwaarden is gelegen in de visie dat het in de informatiemaatschappij om meer dan alleen elektronische handel gaat. Culturele waarden en werkgelegenheid dienen eveneens meegenomen te worden en wel door wettelijke randvoorwaarden.

Het Actieprogramma heeft inmiddels een vervolg gekregen in diverse andere van overheidswege gepubliceerde documenten en rapporten. Zo verscheen op 19 januari 1999 een voortgangsrapport, dat werd besproken in het Comité Interministériel pour la Société de l'Information (CISI).[55] De Franse regering was duidelijk tevreden met de voortgang van de lijnen zoals uitgezet in het Actieprogramma.[56] Een half jaar later deed premier Jospin opnieuw de aankondiging van concrete overheidsactie. Ditmaal gaf hij aan dat de regering voornemens is begin 2000 een wetsontwerp met betrekking tot de informatiemaatschappij aan het parlement voor te leggen.[57] De eerste uitgangspunten van dit wetsontwerp werden duidelijk bij de publicatie van het consultatiedocument *Une société de l information pour tous. Document d orientation* van 5 oktober 1999.[58] Het betreft de volgende drie uitgangspunten:

- de verduidelijking van de rechten en verantwoordelijkheden van eenieder teneinde de vrij online communicatie te waarborgen;
- de democratisering van de toegang tot ICT;
- de zekerheid en betrouwbaarheid bij elektronische transacties.

Op 1 december 1999 sprak premier Jospin nogmaals over het belang van een goed Frans beleid inzake Internet. Hij gaf daarbij aan dat zelfregulering een rol in dit beleid kan spelen, maar vanuit het perspectief van co-regulering: "La corégulation nécessite en effet un dialogue contstant entre tous ses participants".[59] Inmiddels heeft de regering een

53 Conseil d'Etat 1998.
54 De regels die de Internetgemeenschap heeft opgesteld voor goed Internet-gebruik, zie <http://www.ietf.org/rfc/rfc1855.txt>.
55 CISI 1999.
56 Zie ook Lorentz 1999.
57 Jospin 1999a.
58 Strauss Kahn e.a. 1999.
59 Jospin 1999b.

aanzet gegeven tot instelling van een 'organisme de corégulation', voorgezeten door de afgevaardigde Christian Paul.[60]

Wat betreft de inzet van Frankrijk in de diverse internationale gremia stellen we vast dat het land – zoals de meerderheid van de landen – een actieve rol wil spelen bij het vormgeven van het internationale beleid inzake elektronische handel en Internet. Meer specifiek kan worden gewezen op het feit dat de Franse regering in het Actieprogramma van 1998 de noodzaak onderkent om een actievere rol te spelen in de internationale organisaties die betrokken zijn bij de ontwikkeling van technische standaarden die voor Internet van belang zijn.[61]

3.5 Verenigd Koninkrijk

De Britse overheid vindt dat sterk de nadruk op zelfregulering dient te liggen. Aan dit standpunt is onder meer expliciet uitdrukking gegeven in de toespraak uit 1998 van Minister Battle over *Her Majesty s Government Strategy for the Internet* en de op 23 juli 1999 gepubliceerde – maar inmiddels fel bekritiseerde – Electronic Communications Bill.[62]

In principe is pure zelfregulering het uitgangspunt: de taak van de overheid ligt met name in wat wordt aangeduid met de trefwoorden: stimuleren, investeren en informeren. Ten aanzien van 'informeren' acht de Britse regering het voor de ontwikkeling en verdere vormgeving van nationale zelfreguleringsinitiatieven van groot belang dat de Lid-Staten van de Europese Unie onderling hun ervaringen met zelfregulering uitwisselen.

Dat pure zelfregulering niet altijd het uitgangspunt kan zijn wordt overigens ook door de Britse regering erkend. De belangrijkste aanleiding om toch voor regulering van bepaalde onderwerpen te kiezen, is gelegen in de Europese verplichtingen (men wijst in dit verband primair op het terrein van elektronische handel). Hiernaast acht de regering het wenselijk dat ze wetgevingsinitiatieven ontwikkelt op het terrein van illegale en schadelijke inhoud, fraudebestrijding en scholing. Met name dit laatste onderwerp staat hoog op de agenda van de overheid. Immers, "it is vital to have an ICT literate business and workforce".[63] Inmiddels houden het Cabinet Office, het Department of Trade and Industry (DTI) en het Department for Education and Employment zich actief bezig met het ontwikkelen van scholingsinitiatieven en -programma's.[64]

De bovenstaande onderwerpen werden door de Britse regering reeds als onderwerpen voor de reguleringsagenda genoemd in het in 1998 door premier Blair gepubliceerde *Our Information Age*.[65] Concreet stelt hij daar: "The Government will not attempt to replace the private sector – competitive markets will bring the greatest benefits to the economy and consumers alike. But the Government does have an important role to play in five key areas:

- transforming education – to harness new technology so that all can gain knowledge and skills they need for the information age;
- widening access – to ensure that the benefits of the information age are open to all, with no split between information haves and have nots;
- promoting competition and competitiveness – to help harness change and prosper, for the benefit of customers, jobs and the wider economy;
- fostering quality – to ensure that the content of new services matches and exceeds the best available today;

60 Zie <http://www.internet.gouv.fr/francais/textesref/pagsi2/lsi/coregulation.htm>.
61 Conseil d'Etat 1998.
62 Zie <http://www.parliament.the-stationery-office.co.uk/pa/ld199900/ldbills/024/2000024.htm>.
63 S. Saxby, interview.
64 ISI 1999.
65 Blair 1998.

- modernising government – to ensure the Government uses new technology to deliver better, more convenient, services."

Maar ook daar waar de Britse overheid aangeeft dat overheidsbemoeienis noodzakelijk is, blijft ruimte bestaan voor zelfreguleringsinitiatieven. We kunnen stellen dat op deze terreinen naar de mening van de Britse regering sprake is van geconditioneerde zelfregulering. De aanpak van illegale en schadelijke inhoud is hier een goed voorbeeld van. Naast de concrete wettelijke maatregelen stimuleert de regering het opstellen van gedragscodes door de branche. In aanvulling hierop acht ze ook vormen van co-regulering noodzakelijk, bijvoorbeeld waar de informatie- en communicatie-industrie, handhavingsautoriteiten en vertegenwoordigers van ouders en leraren samenwerken in het ontwikkelen van maatregelen om minderjarige gebruikers te beschermen.

Het fenomeen co-regulering als vorm van zelfregulering is een centraal thema in het in september 1999 gepubliceerde rapport *E-commerce@its.best.uk*.[66] In het rapport wordt uitgebreid stilgestaan bij de voor- en nadelen van dit fenomeen voor de regulering van elektronische handel. De belangrijkste drijfveer om te komen tot co-regulering is het gevoel dat de overheid de taak heeft aan zowel consumenten als bedrijven een bepaald niveau van rechtszekerheid en vertrouwen te bieden: "To give consumers and business this trust and thus to facilitate the growth of e-business, an underpinning legal and regulatory framework is essential." Echter, zo wordt vervolgd, juist het doorvoeren van deze wetgeving gaat te langzaam voor de snelle veranderingen in een e-handelmarkt. Aldus biedt co-regulering een alternatief: "Co-regulation is a partnership between government and business designed to put in place an overall framework for e-commerce. Government defines the public policy objectives that need to be secured, but tasks industry to design and operate self-regulatory solutions and stands behind industry ready to take statutory action if necessary".
Als voordelen van co-regulering noemt het rapport:

- flexibiliteit en aanpassingsvermogen;
- tijdsonafhankelijkheid;
- specificiteit en
- "it will help create a distinctive "Based in the UK" brand for UK e-business by giving consumers here and overseas trust in e-businesses based in the UK and enhancing the attractiveness of the UK as a location for e-businesses."

Het rapport staat ook stil bij een belangrijk nadeel, namelijk dat marktpartijen de resultaten van zelfregulering gebruiken als instrument in het oprichten van barrières voor nieuwe markttoetreders. Men geeft vervolgens aan voldoende vertrouwen in het mededingingsrecht te hebben om dergelijke problemen aan te pakken.

Aldus concludeert het rapport dat de voordelen van co-regulering de nadelen verre overstijgen en roept het de regering op om het uitgangspunt van co-regulering expliciet als zodanig te nomen: het "should therefore be the first option for addressing regulatory issues concerning e-commerce." Zo presenteert het rapport de volgende positie als het om de regulering van e-handel gaat: "A recognition of a unique balance between 'light touch' regulation and freedom to innovation expressed through a 'based in the UK' brand, such that:

- Government intervention is only used as a last resort;
- co-regulation is the norm, with a presumption for industry self regulation within a Government backed framework of codes of good practices in the first choice;[67]

---

66 Cabinet Office 1999, gepubliceerd in september 1999 naar aanleiding van een opdracht van Blair daartoe.

67 Ook Australië hanteert dit uitgangspunt. Een interessant voorbeeld aldaar van zelfregulering op basis van door de wet gestelde randvoorwaarden is het op 30 augustus 1999 door de Internet Industry Association (IIA) gepresenteerde ontwerp voor een *Code of Practice for Internet Business*

- disincentives to the use of electronic commerce no longer exist (...); and
- Government is truly 'joined up', with close co-ordination of both policy and its delivery."

Kijken we naar concrete resultaten van zelfregulering in het Verenigd Koninkrijk, dan moet allereerst het systeem van de meldpunten genoemd worden. Bij diverse gelegenheden heeft de Britse regering laten weten dat ze zeer te spreken is over de Internet Watch Foundation.[68] Men benadrukt dat met deze instantie goede ervaringen zijn opgedaan als het om het vergroten van het vertrouwen bij de consument gaat.

Bij het opzetten van diverse zelfreguleringsinitiatieven heeft de Britse overheid direct als stimulator opgetreden. Genoemd kunnen ook worden de oprichting van de Britse Internet Service Providers Association en het TrustUK-initiatief (een keurmerk voor online consumentendiensten op basis van een gedragscode). Deze laatste organisatie zal vanaf maart 2000 een keurmerk verlenen aan e-handelbedrijven die zich aan bepaalde voorwaarden op het terrein van consumentenbescherming en privacy houden.[69]

Ook heeft de Britse overheid opgeroepen tot het gebruik van bepaalde technische beschermingsmaatregelen, zoals PICS[70]. Ten slotte kan in dit verband worden gewezen op de inbreng van de overheid bij de oprichting – in februari 1996 – van The Information Society Initiative (door DTI) om de toepassing van ICT in het midden- en kleinbedrijf te stimuleren.[71]

Inmiddels is begin 2000 Alex Allan aangesteld als E-envoy van de regering. Bij de presentatie van zijn plannen wees ook Allan op de belangrijke rol van de private sector bij het vormgeven van het e-handelbeleid.[72]

Door deskundigen uit het Verenigd Koninkrijk werd er tijdens de internationale workshop op gewezen dat bij het denken over de rol van de overheid nadrukkelijk aandacht besteed moet worden aan de gevolgen voor de handhaving van de gekozen benadering. Hierbij laten ervaringen in het Verenigd Koninkrijk met certificeringsdiensten zien dat overheidsbeleid dat werkt met een systeem van vrijwillige medewerking door de private sector zeer effectief kan zijn: bedrijven en organisaties lijken zich aan dit beleid te willen conformeren omdat dit een concurrentievoordeel kan bieden.

Concluderend stellen we vast dat in het Verenigd Koninkrijk nadrukkelijk ruimte is voor zelfregulering, waarbij het uitgangspunt van pure zelfregulering plaats gemaakt lijkt te hebben voor co-regulering. In deze visie is de rol van de overheid meer dan uitsluitend die van stimulator. Ze heeft een sturende rol in het belang van rechtszekerheid en vertrouwen en stelt daartoe bepaalde minimumeisen. Daarbij is er nadrukkelijk aandacht voor overheidsbeleid dat werkt met een systeem van vrijwillige medewerking door de private sector. Het resultaat is co-regulering, waarbij zelfregulering wordt gecombineerd met "a light touch regulation".[73]

(zie <http://www.iia.net.au>). De Code bevat een verzameling 'best practices' op een groot aantal terreinen: privacy, e-handeltransacties, spamming, illegale en schadelijke inhoud, auteursrecht en eerlijke mededinging door bedrijven. Bedrijven die zich aan de *best practices* houden, kunnen hun weblocatie voorzien van een keurmerk. De IIA acht het van groot belang dat is voorzien in een onafhankelijk systeem van handhaving.

68 Battle 1998 en Blair 1998.

69 Zie <http://www.trustuk.org.uk>.

70 Zie <http://www.dti.gov.uk/CPORN/r3.htm>.

71 Zie <http://www.isi.gov.uk/isi>.

72 Zie *World Internet Law Report*, 2000 nr. 2, p. 6-7. Zie House of Commons 1999 voor de taakomschrijving van deze E-Envoy post.

73 Zie Cabinet Office 1999.

Ten slotte merken we over de positie van het Verenigd Koninkrijk in relatie tot internationale gremia op dat de VK zich een nadrukkelijk voorstander toont van een samenwerking tussen de OESO en de Global Business Dialogue on electronic commerce (GBDe)[74]. Daarbij wordt er op gewezen dat de Europese Commissie actiever moet participeren in de GBDe, om te voorkomen dat deze instantie te zeer wordt gestuurd door bedrijven van buiten de Europese Unie.

3.6 Verenigde Staten

Halverwege de jaren negentig publiceerden de Verenigde Staten diverse beleidsdocumenten waarin een integrale visie op de ontwikkeling van elektronische handel werd gepresenteerd. Nadat in 1996 met de Telecommunications Act het beleid van de Amerikaanse overheid voor het eerst duidelijk werd neergezet, volgden in 1997 de rapporten *Digital Tornado: The Internet and Telecommunications Policy*[75] en het *Framework for Global Electronic Commerce*.[76]

Uit beide beleidsdocumenten sprak het grote belang van zelfregulering. Uitgangspunt van het Amerikaanse beleid was de stelling: primair inzetten op zelfregulering, met de regulering door de overheid achter de hand: "The success of electronic commerce will require an effective partnership between the private and public sectors, with the private sector in the lead." Kortom: pure zelfregulering als uitgangspunt.[77] De overheid stimuleert daarbij de inzet van filtering-, labelling- en andere technieken.

Een blik op de praktijk leert dat vanuit de zelfreguleringsinsteek al vele initiatieven – zoals BBBOnline en recentelijk de *e-mail preference service* van de Direct Marketing branche[78] – tot stand zijn gekomen, en dat de Amerikaanse regering deze ook van harte propageert. Daarbij wordt het reguleringsstandpunt ook gehanteerd in de onderhandelingen in de diverse internationale gremia. De inzet op de Safe Harbor Principles bij de onderhandelingen met de Europese Unie inzake de bescherming van persoonsgegevens is hier een goed voorbeeld van.[79] Ook blijkt deze insteek uit de tijdens diverse bijeenkomsten van internationale organisaties geuite waardering van de Amerikaanse regering voor het werk van de Global Business Dialogue.

Drie jaar na de publicatie van beide documenten blijkt er echter ook een toenemende druk om te komen tot overheidsoptreden op bepaalde terreinen. In het verleden is – al dan niet met succes – wetgeving voorgesteld,[80] er liggen momenteel bij het Amerikaanse Congres wetsvoorstellen over een diversiteit aan onderwerpen (elektronische handtekeningen, online gokken, databanken) en andere onderwerpen staan nadrukkelijk in de belangstelling bij de diverse leden van het Congres (consumentenbescherming en privacy). Tijdens de internationale workshop werd ter illustratie van de reguleringsdrift op zowel federaal als statelijk niveau gewezen op de maar liefst 252 wetten die momenteel in de 50 staten van kracht zijn op het terrein van de elektronische handtekening. Overigens is de verwachting dat vele wetgevingsinitiatieven het komende jaar zullen lijden onder de verkiezingskoorts.[81]

---

74 Zie <http://www.gbd.org>.
75 FCC 1997.
76 White House 1997.
77 Zie ook Department of Commerce 1997.
78 Zie <http://www.the-dma.org>.
79 Zie <http://www.ita.doc.gov/td/ecom/menu1.html> voor informatie over de Safe Harbor Principles.
80 Vgl. de 'Communications Decency Act', de 'Child Online Protection Act' en de 'Child Pornography Prevention Act'.
81 Zie 'Federal Legislative Outlook', *Electronic Commerce & Law Report*, 26 januari 2000, p. 82-83.

De wens toch te komen tot een iets meer sturende rol van de overheid hangt samen met een ander belangrijk uitgangspunt dat gepresenteerd is in de beide uit 1997 daterende beleidsdocumenten. Het betreft de ambitie te komen tot een omvattend en consistent juridisch raamwerk voor de verdere ontwikkeling van de elektronische handel: "Government participation must be coherent and cautious" en "The variety of issues being raised, the interaction among them, and the disparate fora in which they are being addressed will necessitate a coordinated, targeted governmental approach".[82]

Het is op de realisatie van dit uitgangspunt dat recentelijk van diverse zijden kritiek is geuit. Vastgesteld wordt dat de overheid weliswaar actief is bij het stimuleren en ontwikkelen van een diversiteit aan initiatieven, maar dat het bij deze initiatieven ontbreekt aan een uniforme benadering. De overheid dreigt te vallen in precies die valkuil waar het in haar beleidsdocumenten voor waarschuwt, aldus diverse deskundigen. Of, zoals Michael Froomkin het verwoordde op een symposium aan de Universiteit van Berkeley dat in het teken stond van een 'evaluatie' van de beleidsdocumenten uit 1997: "The White Paper is a fundamentally political document consumed by short-term policies and fails to grasp the consequences for governance."[83] Het ontbreekt aan een langetermijnvisie, met als gevolg een beleid van "loose ends and unanswered questions". In toenemende mate wordt opgeroepen tot een meer sturende rol van de overheid om aldus een coherentere benadering veilig te stellen. Het punt van de rechtszekerheid speelt daarbij ook een belangrijke rol. Ook wordt gewezen op de noodzaak om de diverse individuele staten veel meer bij het beleid inzake elektronische handel te betrekken.

Tijdens de internationale workshop werd tevens gewezen op de rol van consumentenorganisaties. Deze laten de laatste tijd in toenemende mate van zich horen en roepen de overheid op te komen met wettelijke regels waarin de belangen van consumenten worden veiliggesteld.

De Amerikaanse literatuur signaleert specifiek ten aanzien van consumentenbescherming drie belangrijke problemen bij zelfregulering:

- zelfregulering heeft onvoldoende effect in een markt waar veel kleine bedrijven opereren en de voorwaarden voor markttoegang laag zijn;
- buitenlandse bedrijven vallen niet onder de handhavingsmaatregelen van de Federal Trade Commission;
- zelfregulering biedt geen oplossing voor de bedrijven op de Internetmarkt die zich niet aan de afspraken houden.

Het is onduidelijk of het een direct gevolg van deze kritiek is, maar president Clinton refereert in zijn Memorandum van 29 november 1999 nadrukkelijk aan de noodzaak te komen tot een uniforme aanpak van wetgevende maatregelen: bij het op te zetten debat over mogelijke juridische barrières voor de verdere ontwikkeling van de elektronische handel is het noodzakelijk "to discuss the potential for consistent approaches to these issues", aldus Clinton.[84]

Een concreet voorbeeld van de tendens is de oprichting van een adviesorgaan bij de Federal Trade Commission dat een nadrukkelijke rol krijgt bij de implementatie van 'privacy principles' bij commerciële weblocaties.[85]

Concluderend stellen we vast dat waar de Amerikaanse regering nog steeds pure zelfregulering als uitgangspunt hanteert, ze er inmiddels ook van doordrongen raakt dat een grotere rol van overheidssturing noodzakelijk is om een uniform en coherent beleid te realiseren, waarmee tevens bepaalde belangen (consumentenbescherming, privacy en

82 White House 1997, p. 30.
83 *Electronic Commerce & Law Report*, 17 maart 1999, p. 241-243.
84 White House 1999.
85 Zie <http://www.ftc.gov>.

rechtszekerheid) kunnen worden veiliggesteld. Ook tijdens de internationale workshop werd deze tendens naar 'co-regulering' onderschreven.

3.7 Vergelijking en conclusie

Een blik op de bovenstaande analyse van de situatie in de diverse landen leert dat de Nederlandse voorkeur voor een inzet op zelfregulering breed in deze landen wordt gedragen. Kijken we meer in detail naar de specifieke invulling van het concept zelfregulering in de onderzochte Europese landen, dan stellen we vast dat het Nederlandse standpunt meer in lijn ligt met de Duitse en Engelse visie op zelfregulering dan met de visie van de Franse regering. Dit laatste land acht het van groot belang dat de overheid specifieke randvoorwaarden aan regulering door de markt stelt.

Wel is een opvallende tendens waar te nemen in de onderzochte landen, die zich oorspronkelijk op het standpunt stelden dat overheidssturing in principe niet is gewenst maar dat de markt het voortouw dient te nemen. We stellen vast dat in al deze landen het besef groeit dat de overheid niet kan volstaan met uitsluitend stimuleren, maar dat het vormgeven van e-handelbeleid en Internetbeleid een taak voor de overheid en de markt gezamenlijk is. 'Co-regulering' is het woord dat in veel recente beleidsdocumenten prominent is terug te vinden. Zelfs in de Verenigde Staten lijkt een tendens waar te nemen waaruit blijkt dat men de mening is toegedaan dat de overheid meer dan voorheen een sturende rol moet gaan spelen bij de vormgeving van het beleid. Uitgangspunt daarbij is het samen optrekken van overheid en markt bij het ontwikkelen van het beleid. Ten slotte stelden we vast dat ook de Franse regering het woord co-regulering inmiddels heeft laten vallen.

Bij de voornoemde constatering is het overigens wel van belang voor ogen te houden dat de term 'co-regulering' in de verschillen landen geen eenduidige invulling krijgt. Ook tijdens de internationale workshop bleek duidelijk dat wat men precies onder dit concept dient te verstaan in belangrijke mate wordt bepaald door wetgevingstraditie en de culturele achtergrond. Kortom, we dienen ons te realiseren dat met dezelfde term wel eens iets anders kan worden bedoeld.

Een blik op de diverse internationale gremia die zich met de beleidsvorming bezig houden, laat zien dat ook hier het uitgangspunt van co-regulering in toenemende mate wordt gepropageerd. Zo heeft de OESO zich tijdens een bijeenkomst in het najaar van 1999 positief uitgesproken over het concept van co-regulering. Alhoewel het verleden heeft laten zien dat de individuele lid-staten zich een voorstander tonen van het – waar mogelijk – doorzetten van hun nationale beleidslijn inzake regulering in de internationale organisaties, hebben ze het uitgangspunt van co-regulering nog niet nadrukkelijk op de internationale agenda geplaatst. De reden daarvan kan zijn gelegen in het feit dat het uitgangspunt pas zeer recent op de nationale beleidsagenda is gezet en nog niet rijp genoeg is voor internationale agendering. Wordt het eenmaal op de internationale agenda geplaatst dan dient men, zoals hiervoor aangegeven, nadrukkelijk rekening te houden met het feit dat het begrip co-regulering per land verschillend wordt ingevuld.

Door diverse regeringen, ten slotte, wordt gewezen op de belangrijke rol die de Global Business Dialogue kan gaan spelen bij het verder vormgeven van het internationale (lees meer specifiek transatlantische) beleid inzake elektronische handel. Daarbij wordt in de Europese landen overigens wel opgemerkt dat men moet oppassen dat de visie van de GBDe niet volledig door het Amerikaanse gedachtegoed wordt beheerst.

Het overzicht leidt tot de conclusie dat het Nederlandse standpunt inzake zelfregulering steun vindt in het buitenland. Wel zal de Nederlandse regering nadrukkelijk oog moeten hebben voor de toenemende populariteit van het concept van co-regulering: de overheid moet meer dan voorheen een sturende rol gaan spelen bij de vormgeving van het beleid. Uitgangspunt hierbij is het samen optrekken van overheid en markt bij het ontwikkelen van het beleid. Daarbij dient ze zich overigens wel te realiseren dat er in de verschillende landen met dezelfde term wel eens iets anders kan worden bedoeld. Wat precies onder dit concept dient te worden verstaan is in belangrijke mate afhankelijk van de wetgevingstraditie en de culturele inbedding.

Een tijdens de internationale workshop ingebracht onderscheid dat van waarde kan zijn bij het denken over de noodzaak van overheidsinterventie is dat tussen regulering waarmee ten behoeve van bijvoorbeeld de rechtszekerheid wordt gepoogd een antwoord te geven op praktische vragen (bijvoorbeeld "kan een elektronische handtekening worden ingezet voor het verrichten van rechtshandelingen?") en regulering waarmee gedrag wordt bä nvloed (bijvoorbeeld "gebruik geen encryptie waarmee opsporingsbelangen wordt gehinderd"). Bij de eerste reden voor regulering zal de markt een positieve houding ten opzichte van overheidsinterventie aannemen, terwijl ze bij de tweede reden de noodzaak daarvan vaak niet zal onderschrijven.

Ten slotte blijkt het aspect van de handhaving van eminent belang bij de discussie over (zelf)regulering. Het succes van (zelf)reguleringsinitiatieven staat of valt met de effectiviteit van de handhaving van de gestelde regels. Bij het denken over de rol van de overheid zal daarom nadrukkelijk aandacht besteed moeten worden aan de gevolgen van de gekozen benadering voor de handhaving. Hierbij laten ervaringen in de Verenigde Staten en het Verenigd Koninkrijk zien dat overheidsbeleid dat werkt met een systeem van vrijwillige medewerking door de private sector effectief kan zijn: bedrijven en organisaties lijken zich aan dit beleid te willen conformeren omdat dit een concurrentievoordeel kan bieden.

4. Handhaving

4.1 Inleiding

De uitdaging die ICT-gerelateerde internationalisering stelt aan het recht heeft twee dimensies. De eerste is hoe om te gaan met het feit dat op handelingen meerdere jurisdicties van toepassing kunnen zijn, zoals bij grensoverschrijdende misdaad en elektronische contracten. Deze dimensie valt relatief eenvoudig aan te pakken door internationale verdragen over rechtsmacht en door internationale samenwerking. De tweede dimensie is echter problematischer: als we vasthouden aan nationale soevereiniteit, hoe kunnen staten dan hun (nationale) wet- en regelgeving handhaven in de internationale informatiesamenleving?

De Nederlandse regering vindt dat de elektronische snelweg geen rechtsvrije ruimte mag worden: in beginsel is het bestaande recht gewoon van toepassing op het Internet (zie hfd. 2). Dit betekent dat de wetten ook gehandhaafd moeten worden.[86]

Gezien het probleem van handhaafbaarheid in de internationale context, moeten daarom op internationaal niveau afspraken worden gemaakt. Deze afspraken kunnen de vorm aannemen van (stimuleren of afwachten van) internationale zelfregulering, internationale verdragen, harmonisatie van materiële rechtsnormen, of afspraken over procesregels (zoals wederzijdse rechtshulp in strafzaken). Dergelijke afspraken kunnen op verschillende niveaus worden gemaakt, zowel in internationaal (VN, OESO) en in regionaal (EU, Raad van Europa) als in bilateraal verband. De Nederlandse regering gaat daarbij uit van een pragmatische aanpak: per handhavingsprobleem per rechtsgebied wordt bekeken wat de meest haalbare en effectieve manier is om in (internationale) handhaving te voorzien.

Op *strafrechtelijk* gebied hanteert de Nederlandse regering daarbij de volgende uitgangspunten:[87]

- De elektronische snelweg mag geen rechtsvrij gebied worden.
- De inbreuk die de handhaving maakt op de privacy van de burger moet steeds worden afgewogen en moet steeds zo gering mogelijk zijn[88].
- Aan de ontwikkeling van de markt moeten zo min mogelijk beperkingen worden opgelegd.
- De kosten voor de gebruiker van de elektronische snelweg die verband houden met handhaving mogen niet onevenredig hoog zijn.

---

86 "Effectieve handhaving op de elektronische snelweg staat voorop: de elektronische snelweg mag geen rechtsvrij gebied worden." Nota WES, p. 10. Ook waar Nederland kiest voor zelfregulering, moet aan de voorwaarde voldaan zijn dat de handhaving van de afspraken voldoende is verzekerd. Nota WES, p. 13.

87 Nota WES, p. 168.

88 Nota WES, p. 10.

Als probleemgebieden van strafrechtelijke handhaving ziet de Nederlandse regering vooral de toereikendheid van het arsenaal aan opsporingsbevoegdheden in een elektronische omgeving, het verzekeren van de mogelijkheid van aftappen van telecommunicatie, de toepassing van opsporingsbevoegdheden op Internet, datamining als opsporingsmiddel, medewerkingsverplichtingen voor Internet-aanbieders en TTP's, en de organisatie en opleiding van politie en justitie.[89]

Op het gebied van *privaatrechtelijke* handhaving ziet de regering de volgende aandachtspunten: bewijskracht van door TTP's vastgelegde elektronische informatie, digitale handtekeningen, de bewijsovereenkomst voor gesloten netwerken, alternatieve geschillenbeslechting en "beslag" op de elektronische snelweg.[90]

In dit hoofdstuk worden de standpunten weergegeven die men in het buitenland heeft over handhaving in algemene zin. De handhavingsaspecten op specifieke terreinen komen gedeeltelijk in de hoofdstukken van deel II aan de orde. Verder wordt ter illustratie in dit hoofdstuk een (niet uitputtend) overzicht gegeven van de terreinen en onderwerpen waarbinnen buitenlandse overheden vooral mogelijke handhavingsproblemen signaleren, met een globale indicatie van de oplossingsrichting die zij daarvoor kiezen.

4.2 Internationale organisaties

Binnen internationale organisaties zijn geen overkoepelende initiatieven bekend om handhaving van ICT-recht in algemene zin te waarborgen. Wel zijn er diverse initiatieven om handhaving op specifieke terreinen te waarborgen.

Zo zijn er de langdurige besprekingen die de Europese Unie en de Verenigde Staten voeren over de Safe Harbor Principles – principes die de privacy, met name de waarborgen van de EU-privacyrichtlijn, in de EU en de VS moeten veiligstellen. De besprekingen vlotten niet bijzonder, gezien de verschillende opvattingen in de VS en de EU over de rol van zelfregulering bij het waarborgen van privacy.[91] Ook de OESO heeft zich intensief beziggehouden met privacy, onder andere in de OESO-richtlijnen voor privacy uit 1981. De ministeriële verklaring over privacy van de OESO-conferentie in Ottawa, december 1998, spreekt uit dat de landen de noodzakelijke stappen zullen nemen om de OESO-richtlijnen over privacy effectief te implementeren, onder andere door te verzekeren "that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress".[92] Op deze ontwikkelingen wordt ook door het bedrijfsleven ingesprongen. Zo heeft de Internationale Kamer van Koophandel in 1998 modelbepalingen opgesteld voor contracten over grensoverschrijdend gegevensverkeer.[93]

Ook op het gebied van de consumentenbescherming geeft een OESO-verklaring aan dat handhaving gewaarborgd moet worden, en wel door "increasing awareness among judicial and law enforcement officials of the need for international co-operation to protect consumers and combat cross-border fraudulent, misleading

89 Nota WES, p. 168-169.
90 Nota WES, p. 169.
91 Zie <http://www.ita.doc.gov/td/ecom/menu1.html> voor informatie over de Safe Harbor Principles.
92 OECD 1998a.
93 Zie <http://www.iccwbo.org/home/statements_rules/rules/1998/model_clauses.asp>.

and unfair commercial conduct".[94] Mede in dat licht heeft de OESO eind 1999 richtlijnen voor consumentenbescherming bij e-handel opgesteld.[95]

Voor de handhaving van het regulerend kader van e-handel kan alternatieve geschillenbeslechting, vooral online varianten daarvan, een belangrijk mechanisme zijn. De concept-EU-richtlijn Elektronische Handel verplicht de lidstaten om wettelijke belemmeringen voor online buitengerechtelijke geschillenbeslechting weg te nemen (artikel 17). Dit "moet ertoe leiden dat een daadwerkelijke functionering van dergelijke mechanismen juridisch en in de praktijk mogelijk is, mede in grensoverschrijdende situaties" (overweging 51).[96] In dit licht is het interessant te vermelden dat een alternatieve-geschillenbeslechtingsprocedure ontwikkeld is binnen de ICANN (Internet Corporation for Assignment of Names and Numbers), de organisatie die wereldwijd verantwoordelijk is voor het toezicht op de uitgifte van domeinnamen. De ICANN heeft drie instanties geaccrediteerd om online-arbitrage over domeingeschillen aan te bieden: het WIPO Arbitration and Mediation Center, eResolution en het National Arbitration Forum.[97]

Ook op strafrechtelijk gebied wordt in diverse fora gediscussieerd over handhaving. Zo heeft de OESO in 1997 'richtlijnen' voor cryptografiebeleid ontwikkeld, die evenwel vanwege het compromiskarakter tussen e-handelsbevordering en opsporing weinig richtinggevend zijn.[98] De Raad van Europa deed in 1995 aanbevelingen voor opsporing in verband met informatietechnologie,[99] waarin onder andere wordt aanbevolen om grensoverschrijdende netwerkzoekingen mogelijk te maken. Om de staatssoevereiniteit daarbij niet te schenden, moet daarvoor wel een ondubbelzinnige wettelijke basis bestaan, die momenteel nog ontbreekt. De Aanbevelingen geven dan ook aan dat er dringend behoefte is aan internationale besprekingen die grensoverschrijdende netwerkzoekingen mogelijk maken. Die besprekingen worden momenteel gevoerd binnen de Raad van Europa, namelijk bij de voorbereiding van het verdrag *Crime in Cyberspace*, dat onder andere een wettelijke basis moet bieden voor grensoverschrijdende netwerkzoekingen en satelliettaps, en dat beoogt een netwerk van centrale contactpunten op te zetten voor de snelle afhandeling van rechtshulpverzoeken (zie verder hfd. 6). Ook de G8 hebben principes gelanceerd voor grensoverschrijdende toegang tot computergegevens (die blijven uitgaan van wederzijdse rechtshulp en dus geen directe benadering van buitenlandse Internet-aanbieders toelaten), en zij hebben een internationaal netwerk van 24 uur per dag bereikbare contactpunten voor informatievoorziening ingesteld.[100] Ook in de Europese ontwerp-overeenkomst over wederzijdse rechtshulp in strafzaken komt grensoverschrijdende opsporing aan de orde: de overeenkomst beoogt grensoverschrijdende onderschepping van telecommunicatie te regelen. Het Europees Parlement heeft in februari 2000 de ontwerptekst echter substantieel geamendeerd,[101]

---

94 OECD 1998b.

95 Zie <http://www.oecd.org/dsti/sti/it/consumer/prod/guidelines.htm>.

96 Gewijzigd Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende bepaalde juridische aspecten van de elektronische handel in de interne markt, COM(1999) 427 def. Zo ook de Conclusies van de Europese Raad in Lissabon, 23 en 24 maart 2000, punt 11. De organen voor alternatieve geschillenbeslechting moeten wel de beginselen in acht nemen uit de *Aanbeveling van de Commissie betreffende de principes die van toepassing zijn op de organen die verantwoordelijk zijn voor de buitengerechtelijke beslechting van consumentengeschillen (98/257/CE)*, <http://europa.eu.int/comm/dg24/policy/developments/acce_just/acce_just02_nl.html>.

97 Zie <http://www.icann.org/udrp/approved-providers.htm>. Vgl. ICANN 1999.

98 OECD 1997.

99 Council of Europe 1995.

100 G8 1999, punten 17 en 19.

101 Zie Asscher 2000, p. 762.

zodat vooralsnog geen overeenstemming bereikt is over de voorwaarden waaronder dit mogelijk zou moeten worden.

Voor strafrechtelijke handhaving in een ICT-omgeving is voorts de telefoontap van eminent belang.[102] Om de aftapbaarheid van telecommunicatienetwerken te verzekeren, hebben diverse initiatieven plaatsgevonden. ILETS (International Law Enforcement on Telecommunications Seminar) is een informeel overleg van onder andere de EU-landen, de VS, Canada en Australië, dat beoogt de samenwerking te verbeteren tussen handhavingsautoriteiten en tapwetgeving op elkaar af te stemmen. De Europese Raad heeft in 1995 een besluit genomen met eisen die lidstaten in acht zouden moeten nemen bij het definiëren en implementeren van maatregelen die de rechtmatige onderschepping van telecommunicatie bë nvloeden.[103] Het betreft hier eisen die opsporingsdiensten stellen om doelmatige en doeltreffende telecommunicatietaps mogelijk te maken. De eisen vertonen opvallende gelijkenis met de eisen in de CALEA-wet van de VS[104] (zie par. 4.6). In dit kader zijn ook nog vermeldenswaard de verwikkelingen rondom Echelon, een wereldwijd aftapnetwerk van de veiligheidsdiensten van de VS, het VK, Canada, Australië en Nieuw Zeeland. Men vermoedt dat dit netwerk de internationale telecommunicatie op grote schaal afluistert en filtert op trefwoorden, waarna vermoedelijk relevante gegevens doorgespeeld worden aan de veiligheidsdiensten van de deelnemende landen (en mogelijk ook aan bedrijven). Het Europees Parlement heeft over Echelon twee rapporten laten opstellen, waarover het in 1998 en in maart 2000 heeft gediscussieerd.[105]

Voor dit onderzoek van bijzonder belang zijn voorts de vele initiatieven binnen de Europese Unie om de strafrechtelijke handhaving te verbeteren. Er zijn talloze formele en informele verbanden en instituties waarbinnen wordt (samen)gewerkt in het kader van toezichthoudende en strafrechtelijke handhaving,[106] zoals Schengen en Europol. Eind 1999 heeft de Europese Raad in Tampere de aanzet gegeven tot instelling van een justitiële tegenhanger van Europol, Eurojust. Ook werd daar gesteld dat het beginsel van wederzijdse erkenning eveneens van toepassing moet zijn op gerechtelijke bevelen die aan het proces voorafgaan, inzonderheid die voor het snel veilig stellen van bewijsmateriaal. Dat kan een ondersteuning bieden voor het legitimeren van grensoverschrijdende netwerkzoekingen en voor de regeling van een 'preservation order' voor buitenlandse Internet-aanbieders die bij het ontwerp-verdrag *Crime in Cyberspace* wordt beoogd. Opvallend is evenwel dat in de conclusies en aanbevelingen van Tampere de nadruk ligt op mensenhandel, georganiseerde misdaad en witwassen, terwijl computer- en Internetcriminaliteit alleen ter sprake komen bij de aanbeveling tot harmonisatie van strafbaarstellingen.[107] Ook ICT-gerelateerde opsporingsbevoegdheden komen niet als zodanig aan de orde. Dit terwijl op de bij uitstek ICT-gerelateerde EU-top in Lissabon (over de kenniseconomie en de informatiemaatschappij) weer geen aandacht is besteed aan opsporing en handhaving.[108] ICT-gerelateerde handhaving valt dus enigszins buiten de boot van de Europese Raad.

---

102 Zie voor een overzicht van internationale initiatieven op dit gebied, Jansen & Janssen 1999.

103 European Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C329/01), WWW <http://www.privacy.org/pi/activities/tapping/eu_tap_resolution_1995.html>. Zie voor een kritische beschouwing over de legitimiteit van dit besluit DPWP 1999.

104 Een latere, ongepubliceerde versie, getiteld 'Declaration of intent', bepaalt dat ondertekenaars contact opnemen met de directeur van de Amerikaanse FBI over de aftapeisen. DPWP 1999, par. A.2.

105 STOA 1998 en STOA 1999.

106 Zie bijvoorbeeld Den Boer 1999 voor een overzicht van de vele vormen van politiesamenwerking.

107 Conclusies van het voorzitterschap, Europese Raad van Tampere, 15 en 16 oktober 1999, SI (1999) 1800.

108 Conclusies van het voorzitterschap, Europese Raad van Lissabon, 23 en 24 maart 2000.

Van geheel andere orde ten slotte, maar voor de handhaving van groot belang, is de internationale samenwerking van meldpunten, die als zelfreguleringsinitiatieven in vele landen zijn opgezet. De Internet Hotline Providers in Europe Association is een samenwerkingsverband van meldpunten voor schadelijke en illegale inhoud in Nederland, Duitsland, Frankrijk, Ierland, Oostenrijk en het Verenigd Koninkrijk, met partners in de Verenigde Staten en Noorwegen. Het bestrijdt met name kinderporno op het Internet door een netwerk van doeltreffende nationale meldpunten op te zetten, nieuwe meldpunten te trainen, het bewustzijn van Internetveiligheid bij Europese Internetgebruikers te stimuleren, en om gemeenschappelijke procedures op te stellen voor meldingen en rapportages van schadelijke en illegale inhoud.[109]

4.3 Duitsland

De Duitse overheid heeft geen uitspraken gedaan of standpunten ingenomen over handhaving van ICT-recht in algemene zin. Op deelterreinen zijn er wel diverse voorstellen die de handhaving moeten verzekeren, waarbij de noodzaak van internationale samenwerking sterk wordt onderschreven

Een terrein waarvan de handhaving Duitsland in het bijzonder zorgen baart is consumentenbescherming. Zelfregulering van aanbieders is internationaal gezien maar beperkt geschikt voor het waarborgen van consumentenbescherming; de mogelijkheden voor gebruikers om in het buitenland recht te zoeken zijn meestal te moeilijk en te duur. Daarom moeten de mogelijkheden voor consumenten vergroot worden om het eigen nationale recht en een toepasselijke rechter in eigen land te kiezen.[110]

Andere onderwerpen waar Duitsland internationale samenwerking of afstemming nodig vindt om handhaving te waarborgen zijn bijvoorbeeld alternatieve geschillenbeslechting[111] en privacy[112]. Anders dan in Frankrijk, het VK en de VS, wordt cryptografie in verband met de opsporing in Duitsland evenwel minder als een probleem ervaren. Weliswaar is er veel gediscussieerd in Duitsland, ook binnen de regering, over mogelijkheden om cryptografie aan banden te leggen, maar tot concrete voorstellen is het nooit gekomen. De Duitse regering spreekt zich sinds 1999 onverbloemd uit voor de vrije verspreiding en stimulering van cryptografie; de overheid legt daarbij veel minder dan Frankrijk en het VK nadruk op de problemen die dat voor opsporing en nationale veiligheid zou kunnen hebben.[113]

4.4 Frankrijk

Een van de algemene Franse uitgangspunten voor het ontwikkelen van een omgeving voor elektronische handel is dat waar nodig wetgeving aangepast moet worden om een kader te scheppen voor elektronische handel dat het vertrouwen wekt van zowel kopers als verkopers. Die wetsaanpassingen moeten dusdanig zijn dat de nieuwe wet- en regelgeving beperkt is en internationale samenwerking bevordert, opdat de

109 Zie <http://www.inhope.org/>.
110 Enquete-Kommission 1998, p. 23. Zie ook Bundesregierung 1999, p. 74-76.
111 Enquete-Kommission 1998, p. 23. Zie ook Bundesregierung 1999, p. 74-76.
112 "Der Datenschutz ist angesichts des globalen Charakters der Netze eine internationale Aufgabe. Ziel ist die Gewährleistung eines weltweit angemessenen Datenschutzniveaus." Bundesregierung 1999, p. 74.
113 Zie Koops 2000.

handhaving van de wet- en regelgeving verzekerd wordt.[114] Frankrijk benadrukt voor handhaving van ICT-recht in algemene zin dus vooral de noodzaak van internationale samenwerking.

Dit gaf premier Jospin ook aan op de slotbijeenkomst van een wereldconferentie van regelinstanties (*régulateurs*) op het Internet: "Bovenal is een nauwere samenwerking in ons aller belang, in het bijzonder om geleidelijk de moeilijkheden te overwinnen die vandaag de dag de toepassing van justitiële beslissingen tegenkomt."[115] Dit geldt overigens niet alleen voor internationale samenwerking: ook nationale toezichthouders moeten samenwerken, omdat geen enkele reguleringsautoriteit alleen de handhaving kan verzekeren. Dit betekent niet dat er een nieuwe toezichthouder moet komen specifiek voor het Internet; eerder moeten alle bestaande autoriteiten beter samenwerken en informatie uitwisselen.[116]

Buiten het genoemde uitgangspunt, heeft Frankrijk geen specifieke standpunten of uitgangspunten over handhaving van ICT-recht in het algemeen. De handhavingsvraag komt alleen aan de orde bij specifieke onderwerpen. Dit speelt bijvoorbeeld bij de toereikendheid van het arsenaal aan opsporingsbevoegdheden op netwerken[117] en de handhaafbaarheid van belastingwetgeving.[118]

Het handhavingsprobleem waar Frankrijk het meest mee heeft geworsteld is het gebruik van cryptografie als belemmering voor de opsporing en bescherming van de nationale veiligheid.[119] Frankrijk was het enige land in de EU dat het binnenlands gebruik van cryptografie sterk aan banden heeft gelegd via een vergunningenstelsel. In de tweede helft van de jaren negentig heeft Frankrijk geprobeerd om via een sleuteldepotsysteem de effectiviteit van telefoontaps en computeronderzoeken te waarborgen, maar dit systeem is niet van de grond gekomen. Gezien het toenemend belang van cryptografie voor de elektronische handel, en gezien de gï soleerde positie die Frankrijk innam binnen de EU, heeft Frankrijk zich gedwongen gezien om het cryptobeleid radicaal te versoepelen en het gebruik van cryptografie vrij te geven, waarvoor in 1999 een belangrijke aanzet is gegeven. Deze versoepeling maakt het handhavingsprobleem voor de strafvorderlijke autoriteiten er echter niet makkelijker op. De Franse regering beoogt dit probleem nu aan te pakken door invoering van een verplichting te ontsleutelen of klare tekst aan te leveren.

4.5 Verenigd Koninkrijk

De Britse overheid heeft geen uitspraken gedaan of standpunten ingenomen over handhaving van ICT-recht in algemene zin. Evenals in Frankrijk is in het Verenigd Koninkrijk de vraag aan de orde geweest of er convergentie moet plaatsvinden van

114 "Any new legislation or regulation must be of a limited nature and favour an international cooperation in order to foster enforcement of existing laws." Lorentz 1998b, onder II-1.2.

115 Jospin 1999b.

116 Jospin 1999b.

117 "Les autorités judiciaires et de police doivent, dans le cadre des procédures pénales, disposer des moyens juridiques pour effectuer des investigations sur les réseaux. C'est une condition indispensable pour lutter efficacement les contenus illicites. […] une disposition legislative doit être envisagée pour permettre d'effectuer ce type d'investigations sur les réseaux." Strauss Kahn e.a. 1999, p. 37-38.

118 "The speed and potential anonymity which are a feature of electronic transactions offer new possibilities for delocalization of taxable items, and even the non-taxation of certain transactions, which are the basic result of the practical difficulty of applying national taxation law over a worldwide network. There is therefore a need to find solutions to these problems so as to protect the interest of countries in terms of income from taxation and to prevent distortions of the marketplace." Lorentz 1998b, onder II-2.1.

119 Zie Koops 2000 voor een overzicht van de Franse wetgeving en beleidsvorming op dit terrein.

reguleringsinstanties (met name van OFTEL en de Independent Television Commission tot een nieuwe 'communications regulator' OFCOM). De regering ziet op korte termijn meer in nauwere samenwerking tussen bestaande toezichthouders dan in het instellen van een nieuwe toezichthouder.[120]

De regering vindt dat de elektronische snelweg geen vrijhaven mag worden. Op deelterreinen leidt dit tot voorstellen die de handhaving moeten verzekeren, terwijl op bepaalde terreinen de handhaving, met name gezien de internationale context, als problematisch wordt ervaren. Daarom wordt de noodzaak van internationale samenwerking onderschreven,[121] evenals de noodzaak van vrijwillige initiatieven van de markt.[122]

Overigens heeft het Verenigd Koninkrijk offline al wel extraterritorialiteit geclaimd voor de strafrechtelijke regeling van sekstoerisme (Sexual Offences (Conspiracy and Incitement) Act 1996), waardoor handhaving in een internationale context aanzienlijk versoepeld wordt. Naar aanleiding van een evaluatie van deze wet zijn eisen opgesteld voor extraterritoriale werking:[123]

1. het betreft een ernstig misdrijf;
2. bewijs en getuigen zijn voorhanden in het VK;
3. er bestaat internationale overeenstemming over de strafwaardigheid;
4. vervolging is nodig omdat de slachtoffers kwetsbaar zijn;
5. vervolging komt de reputatie van het VK ten goede;
6. het gevaar bestaat dat daders vrijuit gaan als het VK hen niet vervolgt.

Deze eisen zijn dermate hoog (met name de derde en vierde eisen beperken het mogelijke toepassingsbereik), dat voor de Internet-context niet valt te verwachten dat het VK voor de internationale handhaving van ICT-(straf)recht zijn toevlucht zal zoeken tot extraterritorialiteit.

De regering van het VK is in het bijzonder bezorgd over de handhaafbaarheid van belastingwetgeving. "E-commerce poses a number of challenges for tax policy and administration: […] designing a tax regime for e-commerce that minimises losses of tax revenues whether because transactions are more difficult to trace […] or because it is difficult to determine the country in which income or profit has been earned and thus to assess which country should get the tax".[124] De belangrijkste voorwaarden voor het waarborgen van de handhaving van belastingwetgeving beschouwt de regering onder andere "international agreement to the implementation of those principles" en "putting in place new arrangements for collecting and enforcing taxes that keep pace with the change in technology."[125]

De parlementaire commissie Trade and Industry ziet evenwel dergelijke internationale afspraken niet snel van de grond komen: "Rapid progress in reaching agreement on how the international tax system should be adjusted to take account of electronic commerce is unlikely, however. The issues are not only complicated but, especially in relation to sales taxes, solutions are hoped for rather than expected to be found."[126]

---

120 House of Commons 1999.

121 Bijvoorbeeld bij de bestrijding van Internetfraude: "International collaboration between regulatory authorities is essential to search out the perpetrators of scams and sharp practices." House of Commons 1999.

122 Zie het vierde principe voor regulering van Internet: "Service Providers should take voluntary action to uphold the law on-line. This works, and has real teeth because the first principle applies [online = offline] and the voluntary action is backed up by the full force of existing law." Battle 1998.

123 Zie het verslag van de internationale workshop in Bijlage IV.

124 Cabinet Office 1999, par. 7.7.

125 Cabinet Office 1999, par. 7.8. Zo ook House of Commons 1999.

126 House of Commons 1999, onder 106.

Evenals Frankrijk is ook de Britse overheid bezorgd over de crypto-problemen voor de handhaving van opsporings- en nationale veiligheidswetgeving.[127] Na herhaalde voorstellen voor sleuteldepotsystemen heeft de regering uiteindelijk in de *Electronic Communications Bill* voorgesteld een bevoegdheid in te voeren om eenieder (inclusief verdachten) te kunnen bevelen een cryptosleutel of klare tekst te overhandigen. Dit voorstel is uitermate controversieel in het VK, gezien de mogelijke inbreuk op het nemo-teneturbeginsel en de voorgestelde omkering van de bewijslast (een weigerende geadresseerde moet aantonen niet te kunnen ontsleutelen, onder dreiging van twee jaar gevangenisstraf). Vanwege de controverse is het voorstel verwijderd uit de Electronic Communications Bill en overgeheveld naar de Regulation of Investigatory Powers Bill, die in februari 2000 bij het Lagerhuis is ingediend.[128]

Voor de handhaving van de bestrijding van schadelijke en illegale inhoud ziet de Britse overheid veel in het marktinitiatief van meldpunten. De Internet Watch Foundation (IWF) is een onafhankelijke organisatie die sinds 1996 illegale inhoud op het Internet bestrijdt, in het bijzonder kinderporno. Behalve een meldpunt voor illegale inhoud, beoogt de IWF ook een classificatiesysteem voor Internet-inhoud te bevorderen, zodat Internetgebruikers in staat zouden zijn te surfen langs op maat gesneden Internet-pagina's.[129] De Britse regering staat achter het initiatief van de IWF als een goed voorbeeld van samenwerking tussen markt en overheid om het recht op het Internet te handhaven.[130]

4.6 Verenigde Staten

De officiële beleidsdocumenten van de Verenigde Staten kennen geen algemene uitgangspunten of oplossingen voor het probleem van handhaving van ICT-recht in een internationale context. Op deelterreinen bestaan echter vele initiatieven die beogen de handhaving te effectueren.

Op strafrechtelijk gebied moet vooropgesteld worden dat de VS traditioneel niet overmatig strikt vasthouden aan het territorialiteitsbeginsel. Naast de weg van bilaterale rechtshulpverdragen (Multi Lateral Assistance Treaties, MLAT's, waarvan de VS bij 13 partij zijn) blijken opsporingsdiensten ook veelvuldig in het buitenland opsporingsactiviteiten te ontplooien in een mengvorm van extraterritoriale strafvordering en (kleine) rechtshulp.[131] Dit maakt dat er mogelijk een minder prangende behoefte bestaat in de VS aan overkoepelende, mondiale afspraken over wederzijdse rechtshulp en grensoverschrijdende ICT-opsporingsbevoegdheden.

De internationale dimensie van ICT-ontwikkelingen baart de VS op strafrechtelijk gebied vooral zorgen bij terroristische activiteiten. Dit komt het meest pregnant naar voren in het cryptografiebeleid van de VS,[132] dat ingegeven is door de vrees dat buitenlandse terroristen door cryptografie aan de afluistercapaciteiten van de National Security Agency en de Central Intelligence Agency ontsnappen. De VS hebben daarom sinds de Koude Oorlog een grote internationale druk uitgeoefend om de export van cryptografie aan banden te leggen, eerst binnen het COCOM-verband en vervolgens binnen het overleg van het Wassenaar-Akkoord. Hiermee hebben de VS hun eigen crypto-beleid geëxporteerd naar de belangrijkste ontwikkelde landen.

---

127 Zie Koops 2000.

128 Zie <http://www.homeoffice.gov.uk/oicd/ripbill.htm>.

129 Zie WWW <http://www.iwf.org.uk/>.

130 Zie Battle 1998 en Blair 1998. Zie ook de uitspraken van diverse ministers tijdens de herlancering van de IWF in januari 2000, WWW <http://www.iwf.org.uk/news/news.html>.

131 Van der Wilt 2000, p. 176.

132 Zie Koops 2000 voor een overzicht van cryptobeleid en -regelgeving in de VS.

Het internationale exportbeleid staat echter in toenemende mate onder druk en wordt stapje voor stapje versoepeld.

Naast de exportwetgeving voor cryptografie, heeft de overheid van de VS ook vele pogingen gedaan om het binnenlands cryptogebruik te reguleren, uit angst voor blokkades van de opsporing. Tot nu toe zijn deze pogingen op niets uitgelopen, waardoor het binnenlands gebruik van cryptografie vrij is gebleven. Het valt ook niet te verwachten dat op korte of middellange termijn wel een binnenlandse cryptoregeling wordt aangenomen.

Ook op het terrein van aftappen van telecommunicatie hebben de VS internationaal het beleid gï nitieerd en gestuurd. De wens om alle telecommunicatie aftapbaar te houden heeft geresulteerd in eisen die zijn vastgelegd in de Communications Assistance for Law Enforcement Act (CALEA) uit 1995, die model heeft gestaan voor aftapbaarheidsregelgeving in andere landen, waaronder het Europese-Raadsbesluit (zie par. 4.2). Bij het implementatietraject van de CALEA wordt uitvoerig gediscussieerd over het eisenpakket waaraan telecomaanbieders moeten voldoen, bijvoorbeeld of ook het doorgeven van locatiegegevens mogelijk gemaakt moet worden.

Meer in het algemeen is er een groots programma voor preventie en opsporing van cybercriminaliteit. Dit beoogt de kritieke infrastructuur te beschermen door onder andere een (omstreden) "Federal Intrusion Detection Network" (FIDNET) op te zetten, een systeem dat een 'cyberalarm' doet afgaan bij aanvallen op computersystemen.[133]

Een ander terrein waarop de VS voorop lopen met het waarborgen van de handhaving is beursfraude. De Security Exchange Commission heeft een Office of Internet Enforcement (OIE) opgezet, dat de activiteiten coördineert van een "CyberForce" van 200 Internet-surveillanten op zoek naar beursfraude op het Internet.[134] Het OIE fungeert ook als contactpunt voor nationale en internationale handhavingsautoriteiten bij Internetzaken.

Op privaatrechtelijk gebied spelen vooral de handhaving van auteursrecht en de ontwikkeling van vormen van alternatieve geschillenbeslechting een rol. Voor de handhaving van auteursrecht worden technische beschermingsmaatregelen als noodzakelijk gezien, zoals Electronic Copyright Management Systems en digitale watermerken. Dergelijke technische maatregelen zijn echter ook technisch te omzeilen. Daarom heeft de overheid van de VS ervoor gekozen om, in navolging van de WIPO en ter implementatie van de WIPO-verdragen uit 1996, de technische maatregelen aanvullende juridische bescherming te geven in de Digital Millennium Copyright Act, die op 12 oktober 1998 werd aangenomen.[135] Deze wet stelt het omzeilen van anti-piraterij-maatregelen strafbaar, alsmede het vervaardigen, verkopen of verspreiden van technologie die is gericht op het omzeilen van anti-copieertechnieken. De wet is voorafgegaan door een hevig publiek debat, waarin ook eerdere wetsvoorstellen zijn gesneuveld. Om tegemoet te komen aan de protesten in dit debat dat de strafbaarstellingen te ver doorsloegen, is in de wet uiteindelijk een uitzondering gemaakt voor anti-anticopieermaatregel-acties ten behoeve van cryptografisch onderzoek, het vaststellen van de interoperabiliteit van producten en het testen van computerbeveiligingssystemen. Ook bestaan er onder omstandigheden uitzonderingen voor bibliotheken, archieven en educatieve instellingen.

Voor de handhaving van civielrecht wordt alternatieve geschillenbeslechting (Alternative Dispute Resolution, ADR), met name bemiddeling (*mediation*) en

133 White House 2000.
134 Zie <http://www.sec.gov/enforce/intrela.htm>.
135 Zie <http://www.gseis.ucla.edu/iclp/dmca1.htm> en <http://www.educause.edu/issues/dmca.html>.

arbitratie, als zeer waardevol gezien.[136] Het zijn effectieve methoden om conflicten op te lossen, die beide partijen meer genoegdoening kunnen schenken en die doelmatiger kunnen zijn dan gerechtelijke afdoening. Het overheidsbeleid is er daarom op gericht om ADR te stimuleren. Het bedrijfsleven is druk bezig met het ontwikkelen van voorstellen voor ADR-mechanismen.[137] Gezien de voorkeur voor zelfregulering, bestaat er vooralsnog alleen een wettelijk kader voor ADR gericht op de overheid. De Administrative Dispute Resolution Act of 1996[138] autoriseert en stimuleert ministeries en overheidsinstanties om ADR te gebruiken. Bij Presidential Memorandum van 1998[139] is een Interagency Alternative Dispute Resolution Working Group (IADRWG) ingesteld, die het gebruik van ADR binnen de federale overheid coördineert, stimuleert en faciliteert.[140] Verder verplicht de Alternative Dispute Resolution Act of 1998 rechtbanken een ADR-programma te ontwikkelen en implementeren.[141]

4.7 Vergelijking en conclusie

In de vier onderzochte landen zijn geen uitgekristalliseerde ideeën te vinden over handhaving van ICT-recht in algemene zin. Met uitzondering van Frankrijk, dat internationale samenwerking noodzakelijk noemt voor handhaving, hebben regeringen geen algemene uitgangspunten voor handhaving geformuleerd, zoals de Nederlandse regering. Dit neemt niet weg dat de vier Nederlandse uitgangspunten grotendeels overeenkomen met de beleidsinitiatieven in de vier onderzochte landen. Men is het erover eens *dat* de elektronische snelweg geen rechtsvrij gebied mag worden, en men is het erover eens dat de vraag *hoe* dat gewaarborgd moet worden in algemene zin problematisch is. Uit de officiële documenten blijkt niet dat men de handhaving op een algemene, overkoepelende manier denkt te moeten, kunnen of willen aanpakken. De pragmatische aanpak van Nederland, om van geval tot geval te bekijken wat de beste aanpak is in internationaal verband om handhaving te verzekeren, komt dan ook in alle onderzochte landen terug.

De terreinen waarover men zich wat de handhaving betreft bijzonderlijk zorgen maakt, verschillen per land. Toch zijn er onderwerpen die in vrijwel alle landen hoog op de lijst staan van (veelal in internationaal verband) aan te pakken handhavingsproblemen. Dit betreft met name de belastingwetgeving, privacy, intellectueel eigendom, het strafvorderlijk instrumentarium op Internet, aftappen en cryptografie, en alternatieve geschillenbeslechting. Op al deze terreinen signaleert men de noodzaak van internationale afstemming en samenwerking, maar in veel gevallen zijn er nog geen uitgewerkte ideeën over hoe die afstemming of samenwerking eruit zou moeten zien, of op welk niveau een gezamenlijke oplossing voor de handhavingsproblemen kan worden gevonden.

Het overzicht leidt tot de conclusie dat de ideeën van de Nederlandse regering over de handhaving van ICT-recht in algemene zin worden gedeeld in het buitenland. Alle overheden realiseren zich dat de handhaving in de hedendaagse internationale context problematisch kan zijn, en dat een internationale aanpak vereist is om handhaving te verzekeren. In algemene zin blijft het daarbij: er bestaan geen ideeën over hoe

136 Zie voor een overzicht <http://www.hg.org/adr.html> en <http://www.usdoj.gov/odr/index.html>.
137 Zie bijvoorbeeld de voorstellen van de United States Council for International Business over online ADR van 17 april 2000, <http://www.uscib.org/policy/adrusgfl.htm>.
138 Zie <http://www.adr.org/law/federal/adminlaw.html>.
139 White House 1998.
140 Zie <http://www.financenet.gov/iadrwg.htm>.
141 Zie <http://www.usdoj.gov/crt/adr/pl105-315.txt>.

handhaving op Internet in algemene zin gewaarborgd kan worden. Van geval tot geval moet onderzocht worden op welk niveau in welk internationaal verband welke aanpak het meest kansrijk en effectief zal zijn om handhaving te verzekeren.

De conclusie van de internationale workshop op dit vlak was dat handhavingsinitiatieven in een internationale context het meest kansrijk zijn als de te waarborgen belangen breed worden gedeeld, zoals in de financiële sector. Op terreinen waar de belangen meer uiteenlopen, in het bijzonder bij het strafrecht, zal de internationale samenwerking die nodig is voor handhaving aanmerkelijk moeizamer en langzamer tot stand komen. Ook hier is het dus raadzaam te beginnen op kleine terreinen waar meer overeenstemming bestaat, zoals bij de bestrijding van kinderporno, waarvoor al een internationaal netwerk van meldpunten actief is.

Volgens de deskundigen op de internationale workshop zijn ook de constructies met nationale contactpunten het meestbelovend om handhaving internationaal aan te pakken. Op privaatrechtelijk gebied kan men denken aan een internationaal netwerk van ombudsmensen of Kamers van Koophandel die als tussenpersoon fungeren bij het oplossen van grensoverschrijdende geschillen. Zij zouden een centrale rol kunnen spelen bij internationale alternatieve geschillenbeslechting. Ook binnen het strafrecht blijkt een internationaal netwerk van nationale contactpunten een constructie die vooralsnog het meest haalbaar en effectief is om handhaving te waarborgen. Een netwerk van contactpunten die 24 uur per dag bereikbaar zijn om direct verzoeken om wederzijdse rechtshulp af te handelen en te coördineren is een oplossing die korte termijn realiseerbaar is en een aanzet kan vormen tot verdergaande vormen van grensoverschrijdende samenwerking.

Deel II – Specifieke onderwerpen

5. Dubbele strafbaarheid

5.1 Inleiding

Ook op het Internet worden strafbare feiten gepleegd. Een voorbeeld daarvan zijn de zogenaamde uitingsdelicten: kinderporno, belediging en smaad, opruiende teksten, discriminatie en racistische uitingen.

Niet in alle landen zijn deze uitingen strafbaar of op een eenvormige wijze strafbaar gesteld, met name vanwege culturele verschillen. Men kan streven naar harmonisatie van strafbaarstellingen, maar dit lijkt voor veel delicten niet of niet op korte termijn mogelijk. Daarom zou men, voorzover de feiten op het Internet worden gepleegd, ook kunnen denken aan het onder omstandigheden loslaten van het beginsel van dubbele strafbaarheid.

Dit beginsel van de dubbele strafbaarheid is verbonden met de statelijke soevereiniteitsgedachte en heeft over het algemeen een belangrijke territoriale component. De kenmerken van het Internet, zoals dematerialisering, deterritorialisering en internationalisering, hebben de Nederlandse regering aanleiding gegeven voor de suggestie om voor de bestrijding van bepaalde delicten op het Internet het vereiste van dubbele strafbaarheid eventueel los te laten. Dit loslaten van het vereiste van dubbele strafbaarheid zou dan een uitzondering zijn op het adagium dat wat online geldt ook offline moet gelden.

Het beginsel van dubbele strafbaarheid houdt in dat alleen internationale rechtshulp in strafzaken wordt verleend als het feit waarvoor de hulp wordt gevraagd zowel in het verzoekende als in de aangezochte staat strafbaar is gesteld. Het gaat bij internationale rechtshulp om (a) rechtshulpverzoeken/rogatoire commissies, (b) uitlevering, (c) overdracht en overname van strafvervolging en (d) overdracht en overname van tenuitvoerlegging van strafvonnissen.

De inzet van de Nederlandse regering is daar waar mogelijk harmonisering van strafbaarstellingen niet af te wijzen. Uniforme strafbaarstellingen lijken echter niet snel en eenvoudig te verwezenlijken. Thans lijkt enkel voor de strafbaarheid van kinderporno een dergelijke 'universele' strafbaarstelling mogelijk.[142]

Voor andere uitingsdelicten gepleegd op Internet kan, nu harmonisatie van strafbaarstelling niet mogelijk is, gedacht worden aan het loslaten van het vereiste van dubbele strafbaarheid. In de ogen van de Nederlandse regering moet dan wel aan een vijftal cumulatieve voorwaarden voldaan zijn. Het vereiste van dubbele strafbaarheid kan losgelaten worden[143] voor (1) informatieverschaffing teneinde het elektronisch spoor te kunnen traceren ten aanzien van (2) vooraf bepaalde ernstige delicten, waarbij

[142] Zie TK, 1999/2000, 23 530, nr. 49, pp. 4-5, Brief van de Minister van Justitie van 23 december 1999 over de voorbereiding binnen de Raad van Europa van het zogenaamde Verdrag Crime in Cyberspace. Zie over dit Verdrag met name hoofdstuk 6.

[143] Nota WES, pp. 8, 116-117, 121 en 205.

(3) het delict gericht moet zijn op de rechtsorde van het verzoekende land. Daarbij wordt wel de eis van (4) reciprociteit gesteld en wordt (5) uitlevering uitgesloten.[144]

5.2 Internationale organisaties

Bij het ontwerp voor een verdrag *Crime in Cyberspace* binnen de Raad van Europa is wel gediscussieerd over het loslaten van het vereiste van dubbele strafbaarheid, maar dit heeft niet geresulteerd in effectieve voorstellen in die richting.[145] Als een van de algemene uitgangspunten (art. 20 van de ontwerptekst) voor internationale samenwerking wordt een basis van uniforme of wederzijdse (*reciprocal*) wetgeving vereist; het vereiste van 'reciproke' wetgeving suggereert niet dat de dubbele strafbaarheid losgelaten zou kunnen of moeten worden.

De formulering van artikel 22, over wederzijdse rechtshulp, suggereert daarentegen dat dubbele strafbaarheid geen vereiste zou hoeven te zijn voor rechtshulp: "Where, in accordance with the provisions of the chapter, the requested Party is *permitted* to make mutual assistance conditional upon the existence of dual criminality (…)" (onze cursivering). Voor één specifiek doel stelt de ontwerptekst zelfs ook voor het vereiste niet te stellen, in artikel 24 lid 3, over het verzoek tot spoedige bewaring (*expedited preservation*) van opgeslagen computergegevens in een andere staat: "For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation, but may be required for the disclosure of the data to the requesting Party." Hierbij staat echter de aantekening: "The Plenary agreed at its 7th meeting (March 2000) that further consideration was necessary on this matter, given that certain delegations expressed their reservation as to the possibility of giving up the requirement of dual criminality." Er is vooralsnog dus geen overeenstemming over het loslaten van het vereiste in dit specifieke geval, en bepaalde staten behouden zich het recht voor het vereiste hier te handhaven. Daar komt bij dat het loslaten van het vereiste alleen voor het *bewaren* van gegevens de verzoekende staat niet zal baten als het vereiste vervolgens blijft bestaan voor het kunnen *inzien* van de gegevens. De ontwerptekst stelt niet ter discussie dat staten bij dit laatste dubbele strafbaarheid kunnen eisen. De verzoekende staat vindt daarom in het verdrag geen effectief middel om gegevens (bijvoorbeeld ter tracering van een digitaal spoor) te verkrijgen als het onderzochte feit in de andere staat niet strafbaar is.

Over het geheel genomen geeft daarom het ontwerp-verdrag *Crime in Cyberspace* geen aanzet tot het loslaten van het vereiste van dubbele strafbaarheid. Hoewel de tekst lijkt te suggereren dat het vereiste niet absoluut zou moeten of hoeven te zijn, bestaat daarover geen eenstemmigheid bij de deelnemende staten.

5.3 Duitsland

Er is geen indicatie dat het loslaten van het vereiste van dubbele strafbaarheid voor uitingsdelicten onderwerp is van overheidsbeleid of beleidsvoorbereiding. Er is geen standpunt, hetzij afwijzend, hetzij steunend, voorhanden.

---

144 De vijf voorwaarden die de Nederlandse overheid stelt aan het loslaten van het vereiste van dubbele strafbaarheid kunnen op zich aanleiding geven tot vragen. Zo is niet exact vast te stellen welk bereik de voorwaarde heeft dat het enkel om informatie zou moeten gaan om het elektronisch spoor te kunnen volgen.

145 Council of Europe 2000.

5.4 Frankrijk

Er is geen indicatie dat het loslaten van het vereiste van dubbele strafbaarheid voor uitingsdelicten onderwerp is van overheidsbeleid of beleidsvoorbereiding. Er is geen standpunt, hetzij afwijzend, hetzij steunend, voorhanden. In *Une société de l information pour tous* van de Franse overheid wordt in het kader van strafrechtelijke onderzoeken eenvoudigweg verwezen naar de huidige procedures.[146]

5.5 Verenigd Koninkrijk

Ook in het Verenigd Koninkrijk is er geen indicatie dat het loslaten van het vereiste van dubbele strafbaarheid voor uitingsdelicten onderwerp is van overheidsbeleid of beleidsvoorbereiding. Er is geen standpunt, hetzij afwijzend, hetzij steunend, voorhanden. Wel wordt om uitingsdelicten te bestrijden de Internet Watch Foundation (IWF) ondersteund (zie par. 4.5).

5.6 Verenigde Staten

Er is geen indicatie dat het loslaten van het vereiste van dubbele strafbaarheid voor uitingsdelicten onderwerp is van overheidsbeleid of beleidsvoorbereiding. Er is geen standpunt, hetzij afwijzend, hetzij steunend, voorhanden.

5.7 Vergelijking en conclusie

Er is geen indicatie te vinden dat in andere landen nagedacht wordt over het mogelijk loslaten van het vereiste van dubbele strafbaarheid. Binnen de Raad van Europa wordt er weliswaar over gediscussieerd, maar over het geheel genomen geeft het ontwerp-verdrag *Crime in Cyberspace* geen aanzet tot het loslaten van het vereiste van dubbele strafbaarheid. Hoewel de tekst lijkt te suggereren dat het vereiste niet absoluut zou moeten of hoeven te zijn, bestaat daarover geen eenstemmigheid bij de deelnemende staten; bovendien wordt het bediscussieerde loslaten van het vereiste beperkt tot het *bewaren* van gegevens in een ander land en strekt het niet uit tot het *overhandigen* van die gegevens, zodat het vereiste in elk geval effectief blijft bestaan.

Ook de discussie tijdens de internationale workshop leverde geen steun op voor het loslaten van het vereiste van dubbele strafbaarheid. De buitenlandse deskundigen toonden zich eerder verbaasd dan gestimuleerd om mee te denken over het idee. Het vereiste van dubbele strafbaarheid leek hen dermate fundamenteel dat er feitelijk geen mogelijkheid zou (moeten) bestaan om er op enige wijze afbreuk aan te doen.[147]

Gegeven het feit dat het onder omstandigheden loslaten van het vereiste van dubbele strafbaarheid internationaal onhaalbaar is, alsmede de bevinding dat harmonisatie van strafbaarstellingen in veel gevallen weinig realistisch is, leidt dit tot de conclusie dat de internationale bestrijding van ICT-criminaliteit zijn toevlucht zal moeten nemen tot samenwerking tussen handhavingsautoriteiten.

---

146 Strauss Kahn e.a. 1999, p. 37.

147 Hierbij kan nog worden opgemerkt dat, met name gezien de doelstelling van het kunnen volgen van het spoor, in landen als de Verenigde Staten en het Verenigd Koninkrijk, waar het op grond van een rechterlijke machtiging doorzoeken van een computer buiten het eigen territoir wel mogelijk is (anders dan in Nederland), een dergelijke vraag naar het loslaten van het vereiste van dubbele strafbaarheid zich waarschijnlijk niet of minder snel voor zal doen.

6. Samenwerking van handhavingsautoriteiten

6.1 Inleiding

Het grensoverschrijdende karakter van elektronische snelwegen brengt met zich mee dat personen die zich fysiek buiten de Nederlandse jurisdictie bevinden relatief eenvoudig strafbare handelingen kunnen verrichten die gevolgen hebben binnen de nationale jurisdictie of die daar zelfs specifiek op zijn gericht. De handhaving van het nationale strafrecht vergt in dergelijke situaties samenwerking tussen Nederlandse en buitenlandse handhavingsautoriteiten. Onder handhavingsautoriteiten worden de verschillende nationale en internationale opsporingsinstanties verstaan.

Samenwerking met buitenlandse autoriteiten is uiteraard niets nieuws. De regels over samenwerking tussen handhavingsautoriteiten zijn vastgelegd in internationale verdragen, waarvan in ieder geval het Europees rechtshulpverdrag en het Beneluxrechtshulpverdrag genoemd moeten worden.[148] Rechtshulp verloopt traditioneel via een rogatoire commissie: het verzoekende land vraagt aan het aangezochte land om bepaalde bevoegdheden te gebruiken ten behoeve van strafvordering in het verzoekende land. Traditionele wegen om rechtshulp te verkrijgen blijken echter niet in alle opzichten te voldoen op de elektronische snelweg. Met name het gebrek aan snelheid speelt opsporingsinstanties op de elektronische snelweg parten. De Nota WES vestigt in dit verband de aandacht op de moeilijkheden die zich voordoen bij het verkrijgen van informatie van netwerkbeheerders in het buitenland. Voor het traceren van hackers is het bijvoorbeeld nodig gegevens te verkrijgen op het moment dat een hacker nog in het systeem 'aanwezig' is. Netwerkbeheerders vervullen hierin een sleutelrol: zij beschikken over bruikbare gegevens (loggings, abonneegegevens, enzovoorts). Echter, tegen de tijd dat zij via de traditionele rechtshulpinstrumenten bereikt worden, zijn vaak belangrijke log-gegevens al gewist, waardoor handhavingsautoriteiten achter het net vissen. De Nota WES ziet de snelheid waarmee handelingen in cyberspace plaatsvinden en de volatiliteit van de sporen die zij achterlaten als hét probleem in de samenwerking tussen handhavingsautoriteiten. De vraag is of dit probleem door een beter gebruik van bestaande rechtshulpinstrumenten kan worden opgelost of dat naar nieuwe oplossingen gezocht moet worden. Gezien de voorliggende problematiek beperken wij ons hier tot de 'kleine rechtshulp'. Uitlevering, overdracht en overname van vervolging en overdracht en overname van de tenuitvoerlegging van vonnissen komen hier niet aan de orde.

148 Europees Verdrag aangaande wederzijdse rechtshulp in strafzaken van 20 april 1959, *Trb*. 1965, 10, en het Beneluxverdrag aangaande de uitlevering en de rechtshulp in strafzaken van 27 juni 1962, *Trb*. 1962, 97.

Nederlandse oplossingen in de Nota WES[149]
De Nederlandse regering acht het wenselijk dat er regels komen over de samenwerking tussen handhavingsautoriteiten.[150] Dat is in het bijzonder nodig om opsporingsbevoegdheden jegens buitenlandse Internet-aanbieders te reguleren en de medewerking van andere landen bij de opsporing te verzekeren.

In het bijzonder moet in het verdrag *Crime in Cyberspace* voorzien worden in mogelijkheden om onmiddellijk informatie bij buitenlandse netwerkbeheerders te verkrijgen. Dat wil zeggen dat opsporingsautoriteiten zich onder omstandigheden rechtstreeks tot buitenlandse netwerkbeheerders moeten kunnen richten, zonder voorafgaande tussenkomst van opsporingsautoriteiten van het land waar de netwerkbeheerder zich bevindt. Rechterlijke toetsing kan dan achteraf plaatsvinden.

6.2 Internationale organisaties

De ministers van de G8 hebben op 10 december 1997 tien beginselen en tien actiepunten vastgesteld ter bestrijding van toptechniekmisdaad (*high-tech crime*).[151] Van de tien beginselen zijn er hier drie van bijzonder belang voor de samenwerking van handhavingsautoriteiten. In de eerste plaats moet wetgeving de bewaring en snelle toegang tot elektronische gegevens mogelijk maken, omdat deze gegevens van kritisch belang zijn voor het succesvol onderzoeken van misdaad (beginsel V). Voorts moeten rechtshulpregimes voorzien in mogelijkheden voor een tijdige garing en uitwisseling van bewijsmateriaal in zaken waarin de internationale toptechniekmisdaad een rol speelt (beginsel VI). Ten slotte behoeft de grensoverschrijdende toegang van handhavingsautoriteiten tot publiekelijk beschikbare (*open source*) informatie niet de toestemming van de staat waar de gegevens zijn opgeslagen (beginsel VII).

Teneinde de aspiraties die in de beginselen besloten liggen waar te kunnen maken zijn actiepunten geformuleerd. Hierbij moet in ieder geval vermeld worden dat een netwerk is opgezet van deskundige rechtshandhavers om een tijdig en effectief antwoord op de grensoverschrijdende toptechniekzaken te verzekeren. Bovendien worden contactpunten ingesteld die 24 uur per dag beschikbaar zijn. De beginselen en actiepunten van de G8 zijn in het algemeen van groot belang, omdat zij (informeel) de agendering in andere internationale fora mede bepalen.

In het kader van de Raad van Europa werkt sinds 1997 een expertgroep – PC-CY – aan een ontwerp voor een verdrag dat voorlopig *Convention on Cyber-Crime* of ook wel *Crime in Cyberspace* wordt genoemd. In april 2000 is voor het eerst een ontwerptekst, de *Draft Convention on Cyber-Crime* (hierna: ontwerp-verdrag) voor consultatie van openbare en private belanghebbende partijen gepubliceerd.[152] Het ontwerpverdrag regelt een groot aantal materiële en strafvorderlijke onderwerpen, zoals het aftappen van gegevensoverdrachten, doorzoeking van computers en inbeslagneming van computergegevens, de bewaring van gegevens, jurisdictie, rechtshulp en de toegang tot publiek-domeingegevens.

Een uitgangspunt van het verdrag is dat strafvorderlijke bevoegdheden in beginsel niet grensoverschrijdend mogen worden toegepast.[153] Dit betekent dat steeds autoriteiten in de desbetreffende staat aangezocht moeten worden. Omdat in

149 Nota WES, p. 116-117.
150 Nota WES, p. 8.
151 Sieber 1998, p. 183-185.
152 Council of Europe 2000.
153 Art. 27 ontwerp-verdrag regelt een uitzondering op dit uitgangspunt: er is geen rechtshulpverzoek nodig voor toegang tot open source gegevens, noch om gegevens te ontvangen van een persoon die zich in een andere staat bevindt en die de gegevens, waartoe hij rechtmatig toegang heeft, vrijwillig verstrekt.

cyberspace rechtshulp vaak met grote spoed vereist is, wordt voorzien in de installatie van nationale centrale contactpunten (art. 23 ontwerp-verdrag). Deze contactpunten zijn 24 uur per dag en 7 dagen per week bemand met deskundig personeel. Zij zijn in staat snel de justitiële autoriteiten te bereiken die moeten worden ingeschakeld voor de gevraagde uitoefening van bevoegdheden. De Nederlandse regering ziet de contactpunten – in wezen het optimaal gebruiken van bestaande rechtshulpinstrumenten – als een stap in de goede richting.

In het ontwerpverdrag is voorts een strafvorderlijke bevoegdheid opgenomen die voor Internetaanbieders van bijzonder belang is: het bewaringsbevel (*preservation order*, art. 16 en 17 ontwerp-verdrag). Dit is een bevoegdheid van Justitie om in het kader van een strafvorderlijk onderzoek de bewaring te bevelen of anderszins te bewerkstelligen van gegevens die in een computersysteem zijn opgeslagen. De bevoegdheid kan slechts worden uitgeoefend als er reden is om aan te nemen dat de gegevens slechts een korte periode bewaard zullen blijven of als er anderszins reden is om aan te nemen dat zij bijzonder kwetsbaar zijn voor verlies of modificatie. Dit is bijvoorbeeld het geval bij aanbieders van telecommunicatiediensten die bepaalde verkeersgegevens om privacy-redenen in beginsel na beëindiging van een oproep moeten verwijderen (of anonimiseren).[154] Ten behoeve van het vergaren van 'verkeersgegevens' over een communicatie moeten de aangesloten staten bovendien voorzien in de nodige (wettelijke) maatregelen om de spoedige bekendmaking aan de autoriteiten te verzekeren van voldoende gegevens om de dienstaanbieders en het pad waarlangs de communicatie plaatsvond te identificeren.

Een bewaringsbevel kan slechts gegeven worden voor gegevens die zijn opgeslagen binnen het territoir van de eigen staat of op een andere plaats waar de eigen staat soevereine bevoegdheden uitoefent. Indien de autoriteiten van de ene verdragsstaat de bewaring wensen van gegevens die in een andere staat zijn opgeslagen, moeten zij zich met een rechtshulpverzoek tot die staat wenden. Bij de voorbereiding van het ontwerpverdrag is met de gedachte gespeeld om verdragsstaten de mogelijkheid te geven zich met een bewaringsbevel of een bewaringsverzoek rechtstreeks tot de houder van de gegevens te wenden.[155] Dit – tijdbesparende – idee heeft het niet gehaald.[156] Er zijn wel enkele andere bepalingen over rechtshulp met betrekking tot het bewaringsbevel in het ontwerpverdrag opgenomen. Zo is uit lid 1 van art. 24 ontwerp-verdrag af te leiden dat het bewaringsbevel een voorlopige maatregel is. De verzoekende verdragsstaat mag de aangezochte verdragsstaat namelijk slechts verzoeken de bewaring te bevelen of te bewerkstelligen, als de verzoekende staat ook van plan is een verzoek in te dienen tot doorzoeking (of een ander vorm van toegang tot gegevens), inbeslagneming (of een andere vorm van zekerstelling) of bekendmaking van de gegevens. Om de verzoekende staat in de gelegenheid te stellen dergelijke opvolgende rechtshulpverzoeken in te dienen, worden de gegevens gedurende tenminste veertig dagen bewaard. De aangezochte verdragsstaat mag de uitoefening van het bewaringsbevel niet weigeren omdat dubbele strafbaarheid ontbreekt, maar de eis van dubbele strafbaarheid mag weer wel aangelegd worden, als het gaat om de bekendmaking van de gegevens aan de verzoekende staat (zie par. 5.2). Er is slechts een beperkt aantal gronden waarop de aangezochte verdragsstaat uitoefening van het bewaringsbevel mag weigeren, namelijk indien de soevereiniteit van de aangezochte staat wordt aangetast, of indien de veiligheid, de openbare orde of andere essentiële belangen worden geschaad.

Indien een verzoek tot uitoefening van het bewaringsbevel betrekking heeft op verkeersgegevens, dan moet de aangezochte verdragsstaat onder bepaalde omstandigheden onverwijld overgaan tot bekendmaking van bepaalde

154 Zie art. 11.5 Telecommunicatiewet.
155 TK 1999-2000, 23 530, nr. 40, p. 9.
156 Art. 23 lid 10 ontwerp-verdrag bevat enige algemene mogelijkheden om rechtshulp te versnellen.

verkeersgegevens (art. 25 ontwerp-verdrag). Dit is het geval indien de aangezochte staat ontdekt dat een derde staat bij de overbrenging van de communicatie betrokken was. De aangezochte verdragsstaat maakt dan voldoende gegevens aan de verzoekende verdragsstaat bekend om de dienstaanbieder en het pad van de communicatie te identificeren. Bekendmaking mag slechts achterwege blijven, als bij bekendmaking de soevereiniteit van de aangezochte staat wordt aangetast, of als de veiligheid, de openbare orde of andere essentiële belangen worden geschaad.

In het kader van de EU wordt gewerkt aan een ontwerpverdrag over wederzijdse rechtshulp. Dit verdrag voorziet – in zijn huidige vorm – in een grensoverschrijdende afluisterbevoegdheid. De Data Protection Working Party heeft een aanbeveling opgesteld over het bewaren van verkeersgegevens door Internet-aanbieders voor opsporingsdoeleinden.[157] De werkgroep meent dat verkeersgegevens in beginsel niet enkel en alleen voor opsporingsdoeleinden bewaard mogen worden en dat nationale wetgeving telecommunicatie- en Internet-aanbieders niet zou mogen verplichten de verkeersgegevens voor een langere periode te bewaren dan nodig is voor factureringsdoeleinden. De werkgroep formuleert als aanbeveling dat de Europese Commissie geschikte maatregelen treft om de bewaarperiode binnen de EU te harmoniseren. De werkgroep lijkt daarbij te denken aan een periode van drie maanden.

In het kader van de Verenigde Naties is een Modelverdrag over wederzijdse rechtshulp in strafzaken opgesteld. Het Modelverdrag regelt onder andere: het eigen toepassingsbereik, de aanwijzing van bevoegde autoriteiten, de inhoud van verzoeken, de weigering van rechtshulp, de bescherming van vertrouwelijkheid, het verkrijgen van bewijs, de beschikbaarheid van vrije en gedetineerde personen voor het geven van bewijs, huiszoeking en inbeslagname, certificatie en authenticatie en de kosten. Een expertgroep beziet hoe het modelverdrag zo actueel en efficiënt mogelijk gehouden kan worden.[158]

6.3 Duitsland

De enquête-commissie van de Bundestag 'Zukunft der Medien in Wirtschaft und Gesellschaft' onderkent de problemen van rechtshulp in een grensoverschrijdende netwerkomgeving en ziet de noodzaak van oplossingen op internationaal niveau. Het geldende recht voor internationale strafvorderlijke samenwerking is te onoverzichtelijk en werkt te traag om een werkelijk effectieve greep op daders die zich in het buitenland bevinden mogelijk te maken. De wetgever dient zich derhalve in te zetten om de internationale rechtshulp te vereenvoudigen en de effectiviteit ervan te verhogen. Dit vergt een internationale samenwerking 'von beispiellosem Ausmaß'.[159] Het federale Ministerie van Justitie zet zich actief in voor de totstandkoming van het Cybercrime-verdrag van de Raad van Europa en neemt deel aan de totstandkoming – in G8-verband – van internationaal afgestemde regels over de vervolging van strafbare feiten begaan in internationale computernetwerken.[160]

Duitsland heeft nog geen standpunt gepubliceerd over *Crime in Cyberspace* of over het rechtstreeks betrekken van informatie van buitenlandse Internet-aanbieders.

---

157 Aanbeveling 3/99 over de bewaring van verkeersgegevens door Internetdienstaanbieders voor wetshandhavingsdoeleinden, goedgekeurd op 7 september 1999, <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp25nl.pdf>.

158 Zie <http://register.aspensys.com/nij/newmeet.htm>.

159 Enquete-Kommission 1998, p. 24.

160 Bundesregierung 1999, p. 45.

6.4 Frankrijk

In verschillende beleidsdocumenten wordt onderschreven dat het grensoverschrijdend karakter van e-criminaliteit een internationale aanpak behoeft.[161] Daarbij wordt gedacht aan samenwerking in het kader van de EU, de Raad van Europa en de G8.

De Conseil d'Etat heeft een uitgebreid standpunt gepubliceerd over versterking van de internationale samenwerking. Hij onderschrijft dat internationale samenwerking noodzakelijk is bij de bestrijding van criminaliteit op het net. De bestaande rechtshulpinstrumenten zijn – naar het oordeel van de Conseil d'Etat – in beginsel toepasbaar in een informatica-context. De bestaande rechtshulpverdragen maken in het algemeen namelijk geen onderscheid naar het type feiten, noch naar de (technische) modaliteiten waaronder zij begaan worden. Niettemin kent de criminaliteit in cyberspace wel specifieke problemen. Deze hangen samen met moeilijkheden rond het traceren van elektronische berichten, de verschillen tussen staten in de toelaatbaarheid van bewijsmateriaal, de toelaatbaarheid van grensoverschrijdende netwerkzoekingen, de internationale implicaties van het verhinderen van de verspreiding van illegale inhoud en de onderschepping van satellietcommunicatie, die naar haar aard vaak vele staten bestrijkt. De Conseil d'Etat concludeert hieruit dat het op zijn plaats is om geheel nieuwe, sui generis-vormen van samenwerking in het kader van rechtshulp te scheppen.

De Conseil d'Etat maakt onderscheid tussen officieus onderzoek en rogatoire commissies. Onder een officieus onderzoek verstaat hij het verrichten van preliminaire onderzoekshandelingen die niet het gebruik van een formele bevoegdheid vergen, maar veeleer het garen van informatie over personen of objecten, zoals iemands precieze identiteit of zijn laatst bekende woonplaats. Teneinde de internationale samenwerking op dit gebied te intensiveren, stelt de Conseil d'Etat voor de informatie-uitwisseling in het kader van Europol en Interpol te versterken.

Rogatoire commissies verlopen doorgaans via de respectieve Ministeries van Justitie. Voor de Internet-omgeving, die zich kenmerkt door snelheid en vluchtigheid, is deze gang van zaken bijzonder ongeschikt. De traditionele rechtshulpinstrumenten dienen dan ook te worden herzien. In dit verband is wel geopperd dat het Openbaar Ministerie of de justitiële politie rogatoire commissies kan uitvoeren zonder voorafgaande controle door een rechter. De Conseil d'Etat doet deze oplossing echter als kwestieus af: de tussenkomst van de rechter is een fundamentele garantie voor de grondwettelijke vrijheden van het individu.[162]

Een daadwerkelijke versnelling van de rechtshulpprocedures zal in internationaal verband tot stand gebracht moeten worden. In afwachting van diepgaandere hervormingen zou het mogelijk gemaakt moeten worden dat rogatoire commissies rechtstreeks van rechter naar rechter gestuurd worden. De resultaten van de onderzoekshandelingen zouden dan ook rechtstreeks van de aangezochte rechter naar de aanzoekende rechter gestuurd moeten worden, in geval van spoed via de fax.

Waar het gaat om het grensoverschrijdend aftappen of afluisteren refereert Frankrijk aan het toekomstige Verdrag van de EU over rechtshulp.[163] Voorts moet in internationaal verband voorzien worden in rechtshulpinstrumenten voor de (netwerk)zoeking en inbeslagneming. De internationale rechtshulp blijft in dit verband het aangewezen mechanisme om justitiële toegang tot gegevens die zich in het buitenland bevinden te verlenen.

161 Lorentz 1998a, Conseil d'Etat 1998 en CISI 1998.
162 Conseil d'Etat 1998, par. 4.3.5.
163 Strauss Kahn e.a. 1999.

6.5 Verenigd Koninkrijk

De Judicial Co-operation Unit van het Britse Ministerie van Binnenlandse Zaken heeft in oktober 1999 een handleiding gepubliceerd over rechtshulp in strafzaken.[164] Deze is met name bedoeld voor buitenlandse autoriteiten die een rechtshulpverzoek in het Verenigd Koninkrijk willen indienen en geeft de huidige stand van zaken weer. Het document gaat niet in op de specifieke problemen die een netwerkomgeving voor rechtshulp oplevert. Voorzover hier van belang kunnen de volgende zaken worden genoemd. Rechtshulpverzoeken kunnen in beginsel in ieder stadium van een opsporings- of gerechtelijk vooronderzoek worden gedaan. Bij rechtshulpverzoeken wordt onderscheid gemaakt tussen verzoeken om 'legal assistance' en verzoeken om 'investigative assistance'. Eerstgenoemde moeten worden gericht aan het Home Office. Het Home Office draagt een meerledige verantwoordelijkheid. Het controleert onder andere of rechtshulpverzoeken voldoen aan de vereisten die het Britse recht en de internationale verplichtingen van het VK stellen. Tevens beziet het Home Office of uitvoering van het rechtshulpverzoek niet ongepast is met het oog op redenen van publiek beleid. Verzoeken die schending van het ne bis in idem-beginsel (dat iemand niet twee keer kan worden vervolgd voor hetzelfde feit) met zich meebrengen worden bijvoorbeeld niet gehonoreerd. Het Home Office is de instantie die verkregen bewijsmateriaal doorgeleidt naar de verzoekende autoriteiten. Verzoeken om 'investigative assistance' kunnen naar het UK National Central Bureau van Interpol worden gestuurd. Dit is onder andere het geval bij verzoeken tot het traceren van bezittingen of tot het verschaffen van gegevens over Britse telefoonabonnees voor opsporingsdoeleinden. De gegevens die over een telefoonabonnee kunnen worden verschaft zijn of haar achternaam en initialen en het adres waar de telefoonaansluiting zich bevindt. Dit zijn namelijk de enige gegevens die Britse telefoonmaatschappijen kunnen aanleveren.

Het Verenigd Koninkrijk kent op dit moment geen strafvorderlijke bevoegdheden die specifiek zien op verkeersgegevens. De verstrekking van gegevens vindt hetzij vrijwillig plaats, hetzij op grond van een door een Crown Court-rechter geautoriseerde Production Order. De Data Protection Act en de Telecommunications Act laten vrijwillige verstrekking voor bepaalde doeleinden toe. De regering heeft in 1999 een wetsvoorstel geformuleerd dat een wettelijke basis geeft aan de verkrijging en verstrekking van 'communications data'. Het gaat om de Regulation of Investigatory Powers Bill, die op 9 februari 2000 aan het House of Lords is aangeboden.[165] De wet ziet zowel op verstrekking in het kader van strafvordering als op verstrekking aan veiligheidsdiensten.

Voor sommige activiteiten – zoals het surfen door openbare informatie op het Internet – zijn geen bijzondere bevoegdheden vereist.[166] Aan formele samenwerking tussen handhavingsautoriteiten komt men dan niet toe. Het surfen over het web kan echter wel plaatsvinden in het kader van een informele samenwerking. Het UK Office of Fair Trading heeft bijvoorbeeld geparticipeerd in een door de US Federal Trade Commission opgezette surfdag: een dag waarop handhavingsautoriteiten van verschillende landen gezamenlijk het web afstruinen op zoek naar frauduleuze weblocaties.[167]

In het rapport *E-commerce@its.best.uk* wordt als aanbeveling geformuleerd: het verbeteren van de technische capaciteiten van rechtshandhavende en regelgevende

164 Judicial Co-operation Unit 1999.

165 Zie <http://www.homeoffice.gov.uk/oicd/ripbill.htm>.

166 Vergelijk TK 1999-2000, 23 530, nr.40, p. 7.

167 *Financial Times* 24 maart 2000, 'Worldwide sweep for internet fraudsters: US oversees action against 1,600 suspect web sites in 28 countries', te vinden op WWW <http://www.globalarchive.ft.com/search-components/index.jsp>.

autoriteiten en de oprichting van een Internet Crime Unit. Dit laatste is een voorstel van de National Criminal Intelligence Service.[168]

De Britse regering speelt een actieve rol in de totstandkoming van het *Crime in Cyberspace*-verdrag.[169] De Britse regering heeft haar standpunt over dit verdrag nog niet naar buiten gebracht. Hetzelfde geldt voor haar standpunt over het rechtstreeks betrekken van informatie van buitenlandse Internet-aanbieders.

6.6 Verenigde Staten

Het Amerikaanse Ministerie van Justitie geeft, in een reactie op een beleidsdocument van de Federal Trade Commission, aan dat de bestaande rechtshulpinstrumenten niet snel genoeg zijn om wezenlijke gegevens veilig te stellen.[170] Bewaring van gegevens is daarmee een van de aandachtspunten in de bescherming van consumenten tegen fraude. US Deputy Attorney General Holder onderkent eveneens de noodzaak van bewaring van gegevens, en hij geeft aan dat privacy-wetgeving niet aan een effectieve rechtshandhaving in de weg mag staan. Dit zou volgens hem kunnen betekenen dat privacy-wetgeving aangepast moet worden in verband met de problemen waarmee de nieuwe technische realiteit de rechtshandhavers confronteert.[171]

De presidentiële werkgroep over onrechtmatig gedrag op het Internet geeft in haar rapport *The Electronic Frontier* van maart 2000 aan dat langs twee sporen naar een verdergaande internationale samenwerking wordt gestreefd.[172] Enerzijds wordt gestreefd naar samenwerking van een meer formele aard in gremia als de Raad van Europa (in het kader van het verdrag *Crime in Cyberspace*) en de G8. Anderzijds worden vormen van informele samenwerking ontwikkeld. Deze informele samenwerking is mogelijk omdat voor sommige activiteiten geen formele bevoegdheden nodig zijn; hierbij kan men bijvoorbeeld denken aan onderzoekingen die zich beperken tot raadplegen van voor het publiek toegankelijke informatie op het web.

6.7 Vergelijking en conclusie

In het buitenland wordt de noodzaak van nauwere samenwerking tussen handhavingsautoriteiten onderkend. Tevens wordt ingezien dat hiervoor ingrijpende aanpassingen in de traditionele internationale rechtshulp nodig zijn. Dit wordt echter vooral gezien als iets waarvoor in internationaal verband oplossingen gezocht moeten worden. Wederzijdse rechtshulp in strafzaken leent zich immers niet goed voor een nationale 'Alleingang'; de term 'wederzijds' geeft dat al aan. Het verlenen van rechtshulp geschiedt op basis van reciprociteit. Vanuit deze achtergrond is verklaarbaar dat de belangrijkste ontwikkelingen in internationale fora plaatsvinden en op nationaal niveau geen definitieve stappen worden gezet in afwachting van ontwikkelingen op het internationale vlak.

Op het nationale niveau beperkt men zich tot kortetermijnmaatregelen, zoals het instellen van permanent bereikbare centrale meldpunten en andere maatregelen die binnen het bestaande rechtskader mogelijk zijn. De Nederlandse wens om gemakkelijker gegevens te kunnen verkrijgen strookt in beginsel met de gedachtevorming in het buitenland. Standpunten over de specifieke wens om

168 Cabinet Office 1999, aanbeveling 10.5.
169 Clarke 1999.
170 Department of Justice 1999, reactie op "topic" 16.
171 Holder 1999.
172 President's Working Group 2000.

gegevens rechtstreeks van buitenlandse Internet-aanbieders te betrekken zijn echter nog niet openbaar gemaakt door buitenlandse overheden.

In het ontwerp-verdrag *Crime in Cyberspace* van de Raad van Europa wordt daarin ook niet voorzien. Wel wordt daarin een nieuwe strafvorderlijke bevoegdheid voorgesteld: het bevel tot bewaring van gegevens (*preservation order*), een bevel aan telecom- of Internet-aanbieders dat gemakkelijk kan worden gegeven en dat het behoud van gegevens verzekert in afwachting van de uitoefening van andere strafvorderlijke bevoegdheden, zoals doorzoeking en 'inbeslagneming'. Voor het bewaren van gegevens die in een andere staat zijn opgeslagen, moet echter nog steeds de weg van het rechtshulpverzoek worden bewandeld – een rechtstreeks verzoek aan buitenlandse aanbieders is afgewezen in het ontwerp-verdrag.

7. Toepasselijk recht op online overeenkomsten

7.1 Inleiding

In de Nota WES constateert de Nederlandse regering dat voor online gesloten overeenkomsten geen specifieke nationale of internationale internationaal-privaatrechtelijke verwijzingsregels bestaan.[173] Het is de vraag of de uniforme verwijzingsregels van het bestaande – offline – internationaal privaatrecht (IPR) uitkomst kunnen bieden. In dit hoofdstuk wordt bezien hoe in andere landen wordt getracht een antwoord op deze vraag te formuleren.

Ter verduidelijking van de problematiek zal eerst een overzicht worden gegeven van de soorten transacties in een online omgeving, omdat de kwalificatie van de rechtshandelingen relevant is voor de vraag van het toepasselijk recht. Vervolgens wordt kort stilgestaan bij de thans vigerende verdragsrechtelijke verwijzingsregels en het standpunt van de Nederlandse regering in de Nota WES. Daarna worden de standpunten van de diverse landen geduid en wordt het standpunt van de Nederlandse regering vergeleken met de vigerende standpunten in de onderzochte landen.

Soorten online overeenkomsten

Bij online overeenkomsten kan een onderscheid worden gemaakt tussen:

- overeenkomsten die online tot stand komen en ook leiden tot het langs elektronische weg leveren van goederen of diensten (strikte online overeenkomsten), en
- overeenkomsten die online tot stand komen maar betrekking hebben op goederen of diensten die langs traditionele weg worden geleverd (indirecte of partiële online overeenkomsten).[174]

Dit onderscheid wordt in de Nota WES niet gehanteerd. Het onderscheid is echter van belang in de context van vragen van toepasselijk recht, omdat bij de eerste categorie sprake is van verschillende rechtshandelingen in een elektronische omgeving, waarbij de daadwerkelijke plaats van de rechtshandeling niet altijd eenvoudig is te duiden, terwijl in de tweede categorie sprake is van feitelijke leveringshandelingen in een bepaald land.

De Nota WES constateert dat op met consumenten gesloten overeenkomsten specifieke beschermingsregels van toepassing zullen kunnen zijn, maar maakt daarbij evenmin onderscheid tussen strikte online overeenkomsten en indirecte online overeenkomsten. Daar komt nog bij dat bij directe online overeenkomsten sprake kan zijn van virtuele actoren, intelligent agents, die namens personen handelen.

---

173 Nota WES, p. 68.

174 Van Esch 1999, p. 14; Prins & Gijrath 2000, p. 3.

Bij gebreke van contractuele rechtskeuze is het mogelijk dat de verwijzingsregels bij strikte online overeenkomsten tot een ander resultaat leiden dan bij indirecte online overeenkomsten, bijvoorbeeld een keuze voor de plaats van totstandkoming van de overeenkomst (dit kan het land van vestiging van de ontvanger van de ontvangstbevestiging zijn) of de plaats van feitelijke levering van het bestelde.

IPR-verwijzingsregels

Het Europees Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomst (EVO)[175] biedt een verdragsrechtelijk systeem van verwijzingsregels. Het is niet beperkt tot bepaalde typen van overeenkomsten, dat wil zeggen dat het van toepassing is op bijvoorbeeld koop of licentie, en op een telefonisch of schriftelijk tot stand gekomen overeenkomst. Daarnaast kent het EVO universele reikwijdte (art. 2 EVO).

Voor online gesloten overeenkomsten geldt allereerst dat deze worden beheerst door het recht dat partijen met inachtneming van art. 3 EVO hebben gekozen. Het EVO hanteert bij gebreke van rechtskeuze als hoofdregel dat het recht van het land van vestiging van de partij die de karakteristieke prestatie levert, de overeenkomst beheerst (art. 4 EVO). Er zijn echter verschillende manieren om te bepalen met welk land een overeenkomst de nauwste band heeft. Hierbij zal de kwalificatie van de overeenkomst een belangrijke rol spelen. In ruime zin kan worden gedacht aan het recht van het land waar de overeenkomst moet worden uitgevoerd, het recht van het land waar de verkoper of dienstverlener is gevestigd, of juist het recht van het land waar de klant is gevestigd, of het land waar de overeenkomst is gesloten. De laatste mogelijkheid laat zich overigens niet altijd goed vertalen naar een online omgeving. De vraag is uiteraard of de 'traditionele' verwijzingsregels zich altijd even goed lenen voor toepassing in een online omgeving.

Bij een consumentenovereenkomst in de zin van art. 5 leden 1, 4 en 5 EVO kan expliciete rechtskeuze er echter niet toe leiden dat de consument geen beroep meer kan doen op de bescherming die hij geniet op grond van dwingende bepalingen van het recht van het land waar hij zijn gewone verblijfplaats heeft. Bij gebreke van een rechtskeuze wordt een overeenkomst met een consument beheerst door het recht van het land waar de consument zijn gewone verblijfplaats heeft, indien de overeenkomst tot stand is gekomen overeenkomstig de voorwaarden genoemd in art. 5 lid 2 EVO.[176] Daarbij wordt een onderscheid gemaakt tussen de actieve en de passieve consument. De passieve consument moet in de EVO-optiek kunnen rekenen op de bescherming van het hun vertrouwde recht. Consumenten die online overeenkomsten sluiten en daarbij keuzes maken, zouden in deze optiek waarschijnlijk als actieve consument dienen te gelden. Dit lijkt, in het licht van bovenvermeld art. 5 lid 2 EVO, niet wenselijk.[177] In Nederland lijkt in ieder geval Webtrader het standpunt in te nemen dat consumenten die online overeenkomsten sluiten, of zij nu als actieve of passieve consument gelden, hoe dan ook hier te lande consumentenbescherming dienen te genieten.[178]

Standpunt Nederlandse regering

In de Nota WES hecht de Nederlandse regering groot belang aan het verduidelijken van de IPR-verwijzingsregels zoals deze van toepassing kunnen zijn op de elektronische snelweg, in dit geval elektronische handel. De Nederlandse regering

175 Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomst, Rome, 19 juni 1980, PB EG 23 (1980) nr. L 266, p. 1.

176 Polak 1998, p. 88.

177 Zo ook Van der Hof 1998, p. 424; Drion 1999, p. 84.

178 Zie <http://www.dedigitaleconsument/webtrader.nl>, met name het standpunt over wet- en regelgeving.

neemt het standpunt in dat het opstellen van specifieke IPR-rechtsregels voor de elektronische snelweg de prioriteit verdient.[179] In de eerste plaats acht zij het wenselijk een ruim geformuleerd kader met regels van IPR op te stellen die van toepassing zijn op online overeenkomsten. Daarbij uit de Nederlandse regering een sterke voorkeur voor afspraken binnen het raamwerk van de Haagse Conferentie.[180]

Vanuit materieelrechtelijk perspectief stelt de Nederlandse regering dat wat offline van toepassing is, ook online dient te gelden. Dat zou dus ook gelden voor online overeenkomsten. Voor online overeenkomsten die onder het EVO vallen, gelden dan de EVO-verwijzingsregels. Over de mogelijke verwijzingsverschillen tussen strikte en indirecte online overeenkomsten laat zij zich niet uit.

7.2 Internationale organisaties

Er zijn geen standpunten bekend van internationale organisaties over het toepasselijk recht op online overeenkomsten. De Raad van Europa concentreert zich op strafrechtelijke aspecten en aansprakelijkheid van Internet-aanbieders en gaat niet op voornoemd vraagstuk in. De meest relevante OESO-documenten[181] gaan hierop evenmin in. De WTO constateert dat internationale afspraken en regels nodig zijn omtrent het recht dat toepasselijk is op elektronische handel, maar er is geen standpunt gevonden over de richting waarheen deze verwijzingsregels zouden moeten gaan. In een aantal landen wordt voorgesteld om een wereldwijd en internationaal raamwerk te ontwikkelen waarbij partijen bij elektronische handel zouden kunnen aansluiten. Daarbij heeft de UNCITRAL-modelwetgeving de voorkeur.[182]

In Europees verband bevat art. 12 lid 2 Richtlijn Verkoop op Afstand van 20 mei 1997[183] rechtsregels die van toepassing zijn op een aantal overeenkomsten die online worden gesloten.[184] Ze bevat een aantal dwingendrechtelijke bepalingen die de consument kan inroepen. Kort gezegd kan rechtskeuze de consument niet van het eigen rechtsstelsel afhouden. Terecht constateert Polak dat deze bepaling moet worden afgestemd met het hiervoor besproken art. 5 lid 2 EVO.[185]

De ontwerp-Richtlijn Elektronische Handel daarentegen voorzag aanvankelijk wel in een regeling maar stelt nu, blijkens overweging 7, niet tot doel te hebben om specifieke IPR-verwijzingsregels binnen de E-handelrichtlijn te geven. Het is een kaderscheppende richtlijn. Art. 9 stelt slechts dat de Lid-Staten zich ervan vergewissen dat de op het contractuele proces toepasselijke rechtsregels het daadwerkelijk gebruik van online overeenkomsten niet beletten, zonder dat het antwoord geeft op de vraag welk recht dan van toepassing is in een specifiek geval. Wel koos de Richtlijn bij de vereisten voor Internet-aanbieders bij hun dienstverlening aanvankelijk voor het beginsel van het land van oorsprong. Aldus moest de Internet-aanbieder voldoen aan de vereisten die in het land van de vestigingsplaats gelden. Inmiddels heeft de Commissie besloten het onderwerp van het toepasselijk recht voor wat betreft consumentenrelaties buiten het kader van de Richtlijn Elektronische Handel te laten.

---

179 Nota WES, p. 6. Daarbij lijkt de Nederlandse regering ook het standpunt in te nemen dat nadere analyse en bepaling van IPR-verwijzingsregels voor online overeenkomsten wenselijk is.

180 Haagse Conferentie voor Internationaal Privaatrecht, 1893. Deze Conferentie heeft de vraag naar toepasselijk recht bij online overeenkomsten inmiddels ook hoog op de prioriteitenlijst staan, zie <http://www.hcch.net/e/events/press01e.html>.

181 OECD 1998c en OECD 1998d.

182 Model Law on Electronic Commerce: With Guide to Enactment 1996 (New York 1997).

183 Richtlijn 4 juni 1997, PB L 144, p. 19.

184 Zie ook Drion 1999, p. 69.

185 Polak 1998, p. 86.

Voor wat betreft *business-to-business* online transacties geldt conform deze Richtlijn het principe van het land van oorsprong.

De door de Nederlandse regering voorgestane aanpassing van de Haagse Conferentie blijkt niet direct spoedig te verlopen. Tijdens een bijeenkomst eind februari 2000 te Ottawa bleek een overeenstemming over het voorliggende concept voor een wijziging van de huidige tekst van de Conferentie verre van haalbaar.

7.3 Duitsland

Ook Duitsland is partij bij het EVO. Op grond van art. 27 Bürgerliches Gesetzbuch staat vrije rechtskeuze in het Duitse stelsel voorop, maar ook in Duitsland kan deze rechtskeuze worden doorkruist door bepalingen die toezien op consumentenbescherming.[186] De specifieke regelgeving op het gebied van elektronische handel, de IuKDG en het Mediendienste-Staatsvertrag, bevat geen specifieke IPR-verwijzingsregels, noch op internationaal, noch op statelijk niveau. Het is niet bekend welk standpunt de Duitse regering ten aanzien van de Haagse Conferentie inneemt. Evenmin is duidelijk of de Duitse regering een voorkeur geeft aan een regeling binnen het kader van de Haagse Conferentie boven een regeling in het kader van enige andere internationale organisatie.

7.4 Frankrijk

Frankrijk is partij bij het EVO maar staat – net als Nederland – een verdergaande mate van harmonisatie van de diverse consumentenbeschermingsregels voor. De Franse regering verbindt daaraan echter niet meteen algemene conclusies over de noodzaak tot het al dan niet vaststellen van nadere regels inzake het toepasselijk recht op online overeenkomsten, al hecht de Conseil d'Etat aan een gebalanceerde aanpak, waarbij zowel met de belangen van de consument als de belangen van verkopers rekening wordt gehouden.[187] Wel wordt het door de Franse regering als een kernvraag aangeduid. De Franse regering geeft niet de voorkeur aan een regeling binnen het kader van de Haagse Conferentie boven andere internationale gremia. Zij geeft daarentegen de voorkeur aan een sectorale aanpak van de problematiek. Verder stelt de Franse regering dat niet zonder meer een regeling van IPR-verwijzingsregels tot stand hoeft te worden gebracht waarbij online en offline dezelfde beginselen zouden worden gehanteerd.

7.5 Verenigd Koninkrijk

Het Verenigd Koninkrijk heeft het EVO in de nationale wetgeving gä mplementeerd.[188] Er is geen verschil geconstateerd tussen art. 5 lid 2 EVO en de

186 Over de specifieke uitwerking hiervan is weinig gevonden, zie bijvoorbeeld Linklaters & Alliance 1999, p. 99.

187 Conseil d'Etat 1998.

188 Contracts (Applicable Law) Act 1990, zie <http://www.hmso.gov.uk/acts/summary/01990036.htm>. Deze wet bevat geen specifieke bepalingen voor online overeenkomsten maar kan wel daarop worden toegepast.

implementatie van de Richtlijn Oneerlijke Bedingen,[189] terwijl de Richtlijn Verkoop op Afstand nog niet is geïmplementeerd .

Het is niet gebleken of de Britse regering net als de Nederlandse een systeem voorstaat waarbij een supranationaal juridisch raamwerk voor rechtskeuze bij online overeenkomsten wordt uitgewerkt, maar de verwachting is dat de regering hierover wel een standpunt zal formuleren.[190]

Ten aanzien van de Haagse Conferentie heeft de Britse regering (nog) geen standpunt ingenomen. Evenmin heeft de Britse regering een strikte voorkeur voor regeling binnen deze Conferentie en houdt het regeling binnen andere gremia, zoals OESO, WIPO, UNCITRAL, WTO en de EU open. Er is in algemene zin ondersteuning voor het adagium van de Nederlandse regering dat hetgeen offline van toepassing is (zie par. 2.5), ook online dient te worden toegepast, maar het is niet duidelijk of dit ook bij het toepasselijk recht op online overeenkomsten wordt gehanteerd.

7.6 Verenigde Staten

De VS staan nadere uniformering voor in het kader van de ontwerp-UNCITRAL-regelgeving voor elektronische handel.[191] De UNICTRAL-regeling bevat echter geen opinie of verschaft geen inzicht in de IPR-verwijzingsregels voor online overeenkomsten. Het vraagstuk van toepasselijk recht op internationale online overeenkomst lijkt op federaal beleidsniveau in de VS niet te spelen.

In de Verenigde Staten doet zich nog de kwestie voor dat het toepasselijk recht op online overeenkomsten per staat kan worden bepaald. Er is jurisprudentie die verwijzingsregels geeft. De tendens lijkt dat rechtskeuze en verwijzing nauw samenhangen met rechtsmacht.

7.7 Vergelijking en conclusie

In vergelijking met de onderzochte landen lijkt het standpunt van de Nederlandse regering, inhoudende dat het de voorkeur verdient om IPR-verwijzingsregels terzake van het recht toepasselijk op online overeenkomsten zo spoedig mogelijk binnen het raamwerk van de Haagse Conferentie te regelen, vooralsnog in de onderzochte landen niet te worden gedeeld. In de VS lijkt het vraagstuk op federaal niveau geen rol te spelen in de beleidsvorming. In Duitsland en het Verenigd Koninkrijk zijn hierover geen standpunten gevonden, terwijl Frankrijk een afwijkend standpunt heeft geformuleerd. In deze landen wordt vooralsnog aanknoping gezocht bij de bestaande regels van het EVO. Het lijkt erop dat men de afstemming tussen art. 5 lid 2 EVO en de rechtskeuze-bepalingen in de Richtlijn Oneerlijke Bedingen en de Richtlijn Verkoop op Afstand niet heeft doen plaatsvinden, al zijn evenmin indicaties gevonden dat deze Richtlijnen tot andere of tegenstrijdige verwijzingsregels zullen leiden.[192] We kunnen concluderend stellen dat Nederland ten aanzien van het recht dat toepasselijk is op online overeenkomsten meer oog heeft voor een mondiale aanpak dan de onderzochte landen.

---

189 The unfair terms in consumer contracts regulations 1994 (SI 1994 No. 3159). Regulation 7 bevat een rechtskeuze-clausule, zie <http://www.dti.gov.uk/access/unfair/part8.htm>.

190 Zie bijvoorbeeld de positie ten aanzien van de Draft Convention on the Protection of Adults, <http://www.scotcourts.gov.uk/forms/draft_2.htm>.

191 UNCITRAL Model Law on Electronic Commerce, General Assembly Resolution 51/162, 16 december 1996, met additioneel art. 5bis, 1998, <http://www.uncitral.org>.

192 Zie hierover ook Van der Hof 2000.

Daarbij dient wel te worden aangetekend dat de door de Nederlandse regering voorgestane aanpassing van de Haagse Conferentie niet direct spoedig lijkt te verlopen. Tijdens een bijeenkomst eind februari 2000 te Ottawa bleek een overeenstemming over het voorliggende concept voor een wijziging van de huidige tekst van de Conferentie verre van haalbaar.

8. Civiele aansprakelijkheid van Internet-aanbieders

8.1 Inleiding

Internet-aanbieders verschaffen toegang tot het net. Zij vervullen een intermediaire functie die wordt omschreven met termen als toegangs-, dienst- of netwerkaanbieder. Het zelf verschaffen van informatie is niet kenmerkend voor hun rol. Dat neemt niet weg dat zij soms wel betrokken kunnen zijn bij de informatie die via hun systemen verspreid wordt. In het algemeen wordt de informatie echter verschaft door derden, dat wil zeggen door Internetgebruikers. Hoewel de meeste gebruikers het net gebruiken voor de verspreiding van volstrekt legale inhoud, blijken enkele gebruikers de geboden faciliteiten te misbruiken voor de verspreiding van onrechtmatige inhoud. De gebruikers die die informatie op het net plaatsen (de zogenaamde inhoudsaanbieders) zijn uiteraard in de eerste plaats verantwoordelijk voor de inhoud. Slachtoffers van onrechtmatige inhoud (zoals auteursrechthebbenden, slachtoffers van smaad of schendingen van privacy) zouden hen dan ook civiel aansprakelijk kunnen stellen. In de praktijk blijkt het vaak moelijk om inhoudsaanbieders (in rechte) aan te spreken. Daarom richten slachtoffers hun juridische pijlen vaak mede op de Internet-aanbieder. Deze kan onder omstandigheden zelf civielrechtelijk aansprakelijk worden gehouden voor zijn bijdrage aan de verspreiding. Daarnaast verkeert de Internet-aanbieder feitelijk in een unieke positie waar het gaat om het traceren en identificeren van inhoudsaanbieders. Hij beschikt immers over gegevensbestanden (zoals abonnee- en log-gegevens), over technische expertise en over goede contacten met andere Internet-aanbieders. De Internet-aanbieder neemt daarom een sleutelpositie in voor de burger die zijn recht zoekt als hij slachtoffer is geworden van onrechtmatige inhoud.

Niettemin blijkt het vinden van daadwerkelijke rechtsbescherming op het Internet vaak moeilijk. Dit is in het bijzonder zo wanneer de Internet-aanbieder en het slachtoffer zich niet in hetzelfde land of dezelfde jurisdictie bevinden. Dan doemen aanvullende problemen op die samenhangen met vragen over de aansprakelijkheid van Internet-aanbieders in het buitenland. Onder welke voorwaarden kan een Internet-aanbieder in het buitenland aansprakelijk worden gesteld? Tevens is van belang in hoeverre Internet-aanbieders in het buitenland in staat, bereid, bevoegd of verplicht zijn hun medewerking te verlenen aan pogingen inhoudsaanbieders te traceren en te identificeren.

In dit hoofdstuk beperken we ons tot drie vormen van onrechtmatige inhoud: auteursrechtinbreuk, smaad en schending van privacy. Tevens beperken we ons tot het civiele recht. Aan de beperking tot het civiele recht liggen twee redenen ten grondslag. In de eerste plaats is het materiële strafrecht meer dan het civiele recht gericht op het hooghouden van bepaalde waarden. Het is daarmee meer cultureel bepaald dan het civiele recht. In de grenzeloze context van het Internet levert het strafrecht dan ook meer stof voor conflicten op. Het vraagstuk van de strafrechtelijke

aansprakelijkheid van Internet-aanbieders in internationaal perspectief is dan ook tamelijk problematisch. Wij bekijken hier of er in het civiele recht – waar de discrepanties in materiële normstelling minder spelen – een gemeenschappelijke noemer gevonden kan worden voor de aansprakelijkheid van Internet-aanbieders. Men kan dit zien als een toepassing van een strategie om in internationaal verband overeenstemming te bereiken over onderwerpen waarover verschil van inzicht bestaat: men begint met regulering van die onderwerpen waarover redelijk gemakkelijk overeenstemming bereikt kan worden en bouwt dit later langzaamaan uit naar onderwerpen die moeilijker liggen. Een tweede reden om de civiele aansprakelijkheid hier te behandelen is gelegen in de omstandigheid dat een civiele partij geen strafvorderlijke dwangmiddelen tot zijn beschikking heeft om de identiteit van een inhoudsverschaffer te achterhalen. Dat doet de vraag rijzen of hij wel voldoende mogelijkheden heeft om tot actie over te gaan.

Oplossing van de Nota WES
Over de civiele aansprakelijkheidspositie van Internet-aanbieders en de grensoverschrijdende aspecten van dit vraagstuk heeft de regering het volgende standpunt ingenomen. Puur nationaal bezien is er geen reden om in een aparte regeling voor de civiele aansprakelijkheid van Internet-aanbieders te voorzien. Het Nederlandse onrechtmatige-daadsrecht is voldoende techniek-onafhankelijk, en de open structuur van de norm laat alle ruimte voor nadere ontwikkeling van het vraagstuk door de rechter. Niettemin onderschrijft de regering het standpunt van de Europese Commissie dat op het internationale vlak een verzameling gemeenschappelijk beginselen vastgelegd moet worden om een *level playing field* te scheppen.[193] De regering acht het immers van belang dat er een goede internationale regeling bestaat voor de privaatrechtelijke aansprakelijkheid van tussenpersonen. Zij steunt dan ook de poging van de Commissie om regels te maken over de aansprakelijkheid van dienstaanbieders.[194] Dit neemt overigens niet weg dat zij op punten wel bezwaren heeft tegen de regeling die neergelegd is in de voorgestelde elektronische-handelsrichtlijn.[195] De Minister van Justitie plaatst een vraagteken bij de hardheid van het onderscheid dat de richtlijn maakt tussen de verschillende categorieën van dienstaanbieders: aanbieders van toegang, caching-diensten en hostdiensten. Bovendien vraagt hij zich af of het verstandig is op voorhand bepaalde categorieën dienstaanbieders (met name toegangsaanbieders) van aansprakelijkheid uit te sluiten, ongeacht hun wetenschap van onrechtmatige inhoud.

De regering is voornemens in internationaal verband actief aandacht te vragen voor het belang van de burger (het slachtoffer) om een elektronisch spoor te volgen en daders te traceren.

8.2 Internationale organisaties

In de Ministeriële verklaring van de Conferentie van Bonn (6-8 juli 1997) is een aantal beginselen met betrekking tot de verantwoordelijkheid van tussenpersonen vastgelegd.[196] Zo moet de verantwoordelijkheid in duidelijke rechtsregels worden gedefinieerd. Die regels dienen te berusten op gemeenschappelijke beginselen, opdat voor eenieder gelijke voorwaarden gelden. De verklaring legt een basis voor differentiatie van verantwoordelijkheid naar de verschillende functies van actoren. Zo

193 TK 1998-1999, 25 880, nr. 7.
194 TK 1998-1999, 25 880, nr. 7, p. 9.
195 TK 1998-1999, 25 880, nr. 7, p. 10.
196 Zie <http://www2.echo.lu/bonn/finalnl.html>.

onderscheidt de verklaring zelf de volgende categorieën: producenten en verspreiders van inhoud, netwerkexploitanten en toegangverschaffers, en hostdienstaanbieders.

Ten slotte dienen de verantwoordelijkheidsregels de vrijheid van meningsuiting te respecteren, de openbare en particuliere belangen in acht te nemen en de betrokken actoren niet te zwaar te belasten.

In de elektronische-handelsrichtlijn van de EU wordt een horizontale regeling voor de aansprakelijkheid van Internet-aanbieders neergelegd.[197] De regeling geldt zowel voor strafrechtelijke als voor civielrechtelijke aansprakelijkheid en omvat in beginsel alle typen delicten. Ook hier wordt gedifferentieerd naar de functies van de actoren. De actor die zich beperkt tot "mere conduit" is bevrijd van aansprakelijkheid, als hij aan een aantal puur feitelijke voorwaarden voldoet, ongeacht zijn wetenschap. De aanbieder van hostdiensten is niet aansprakelijk, indien hij geen wetenschap heeft van de onrechtmatige inhoud (of van omstandigheden die daarop duiden) of indien hij de betreffende informatie prompt verwijdert of de toegang daartoe onmogelijk maakt, zodra hij op de hoogte geraakt. De aanbieder van cache-diensten moet aan een groot aantal zorgvuldigheidsverplichtingen voldoen om aan aansprakelijkheid te ontsnappen. Geen van de voornoemde actoren is verplicht proactief te controleren op onregelmatigheden in de informatie die voorwerp is van hun dienstverlening. De elektronische-handelsrichtlijn bevat geen verplichtingen voor de actoren tot identificatie van inhoudsverschaffers.

De EU heeft een groot aantal beleidsdocumenten uitgevaardigd over de bescherming van minderjarigen tegen illegale en schadelijke inhoud op het Internet.[198] Voor informatie die niet illegaal is maar wel schadelijk kan zijn voor minderjarigen wordt een andere benadering gekozen dan voor illegale informatie. Minderjarigen moeten door technische en organisatorische maatregelen worden afgeschermd van deze informatie. Het kan daarbij zowel gaan om toegangscontroles bij de bron (de informatie) als om – door ouders te installeren – filterprogrammatuur die op browserniveau ingrijpt. Het gebruik van filterprogramma's vergt een enorme inspanning op het gebied van waardering (rating) van inhoud.

8.3 Duitsland

Aansprakelijkheid van Internet-aanbieders

Duitsland kent sinds 1 augustus 1997 een horizontale regeling over de aansprakelijkheid van dienstaanbieders. Deze regeling is neergelegd in het federale Teledienstegesetz en het Mediendienste-Staatsvertrag. Zij maakt onderscheid naar de verschillende functies die dienstaanbieders vervullen. Dienstaanbieders zijn voor hun eigen inhoud volgens de geldende regels aansprakelijk. Voor het aanbieden van vreemde inhouden zijn dienstaanbieders slechts aansprakelijk indien zij daarvan kennis hebben, zij technisch in staat zijn het gebruik ervan te verhinderen en een dergelijke verhindering redelijkerwijze van hen verlangd kan worden. Dienstaanbieders zijn niet aansprakelijk voor inhoud van derden waartoe zij slechts toegang verlenen. Beroepsmatig opererende dienstaanbieders zijn verplicht hun naam en adres te vermelden bij hun dienstenaanbod. Verenigingen moeten ook de naam en het adres opgeven van degenen die vertegenwoordigingsbevoegd zijn. Onder dienstaanbieders vallen echter niet informatie-aanbieders bij wie de redactionele vormgeving ten behoeve van de openbare informatievoorziening op de voorgrond staat (bijvoorbeeld

197 Gewijzigd Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende bepaalde juridische aspecten van de elektronische handel in de interne markt, COM(1999) 427 def. (hierna: elektronische-handelsrichtlijn).

198 Voor een overzicht van Europese beleidsdocumenten op dit gebied, zie <http://www2.echo.lu/legal/en/internet/internet.html>.

verschaffers van opiniërende inhoud). Aanbieders van beursinformatie of aanbieders van waren of diensten zijn daarentegen wel dienstaanbieders.

Identificatie van inhoudsaanbieders
De parlementaire enquête-commissie 'Zukunft der Medien in Wirtschaft und Gesellschaft' onderkent de identificatie-problemen die ontstaan door het gebruik van pseudoniemen, anoniemen en encryptie-technieken.[199] Zij ziet het beperken van de mogelijkheden om encryptie-technieken te gebruiken niet als oplossing, vanwege de vele ontwijkingsmogelijkheden van een dergelijke beperking en vanwege de (privacy-)nadelen voor burgers en ondernemingen. Wat betreft anoniemen bestaat een regelrecht conflict tussen privacy en rechtshandhaving. In hoeverre dit conflict bevredigend kan worden opgelost hangt af van de techniek. Mocht het echter tot een beperking van het gebruik van anoniemen komen, dan moet in ieder geval het gebruik van pseudoniemen gewaarborgd blijven. Gegevens die een relatie leggen tussen iemands identiteit en diens pseudoniem moeten goed beveiligd worden tegen onbevoegde kennisname. Het standpunt van de Duitse regering over wat van Internet-aanbieders verwacht mag worden met betrekking tot identificatie van inhoudsaanbieders is niet bekend.

Het Bundeskriminalamt (hierna: BKA) heeft onderzoek verricht naar de criminaliteitseffecten van de opkomst van e-handel en de gevolgen die dit voor de politietaak heeft. In haar rapport *Electronic Commerce. Markt der Zukunft auch für Kriminelle?* beveelt zij onder andere aan de anonimiteit bij e-handel te verminderen.[200]

Internationale regulering
Oplossingen voor de hiervoor genoemde problemen met betrekking tot identificeerbaarheid moeten volgens de enquête-commissie bij voorkeur in internationaal verband tot stand komen.[201]

Grensoverschrijdende aspecten
Duitsland heeft in het verleden wel pogingen ondernomen om via toegangsaanbieders greep te krijgen op informatie die in het buitenland wordt aangeboden. Deze pogingen zijn niet succesvol gebleken. In 1998 is de directeur van CompuServe Duitsland (Felix Somm) veroordeeld wegens de verspreiding van kinderpornografie. CompuServe Duitsland gaf toegang tot nieuwsgroepen van haar Amerikaanse moedermaatschappij. De veroordeling heeft veel beroering gewekt in Duitsland, en Somm is onlangs in hoger beroep vrijgesproken.[202] De Duitse netwerkaanbieder DFN heeft in 1997 op instigatie van Duitse justitiële autoriteiten enige tijd de toegang (vanuit Duitsland) geblokkeerd tot alle weblocaties die door de Nederlandse Internet-aanbieder Xs4all werden aangeboden. De reden hiervoor was dat een van de locaties een in Duitsland verboden aflevering van het blad Radikal bevatte.[203] DFN heeft na verloop van tijd haar blokkade gestaakt, omdat haar duidelijk was geworden dat de blokkade niet meer effectief was als gevolg van de vele spiegelweblocaties die waren ontstaan.

199 Enquete-Kommission 1998, p. 24.
200 Zie <http://www.bka.de/pressemitteilungen/2000/pm000224.html>.
201 Enquete-Kommission 1998, p. 24.
202 Zie <http://www.somm-case.de>.
203 Zie <http://www.xs4all.nl/spotlight/blokkade_e.html>.

8.4 Frankrijk

Aansprakelijkheid van Internet-aanbieders
Op dit moment kent het Franse recht geen aparte regeling voor Internet-intermediairen. In het kader van het – nog lopende – wetgevingsproject tot herziening van wet nr. 86-1067 van 30 september 1986 over de communicatievrijheid, heeft de parlementariër Patrick Bloche een amendement ingediend, waarmee een regeling over de aansprakelijkheid van Internet-aanbieders aan dit wetsvoorstel wordt toegevoegd. Volgens dit amendement zijn technische tussenpersonen bevrijd van aansprakelijkheid voor informatie die zij transporteren of aanbieden (*hosten*), mits zij niet hebben bijgedragen aan de schepping of voortbrenging van die informatie. Tevens moeten opslagaanbieders (*hosting providers*) de toegang tot informatie verhinderen, indien zij daartoe door justitie zijn aangemaand. Het amendement is door de Assemblée Nationale aangenomen bij de behandeling van het wetsvoorstel in eerste lezing. Tijdens de verdere parlementaire behandeling is de regeling zoals Bloche die in zijn amendement had neergelegd, sterk gewijzigd en aangescherpt. Er bestond onder andere bezwaar tegen het feit dat een Internet-aanbieder die op de hoogte is van onrechtmatige inhoud daartegen niet hoeft op te treden, zolang hij door justitie niet is aangemaand.[204] Per 23 maart 2000, na behandeling door de Assemblée Nationale in tweede lezing, is de stand van zaken, geparafraseerd weergegeven, als volgt.[205] De regeling maakt onderscheid tussen de aanbieder van toegang en de aanbieder van opslag. Eerstgenoemde biedt toegang tot online communicatiediensten, anders dan privé-correspondentie. Laatstgenoemde verzorgt de opslag ten behoeve van beschikbaarstelling aan het publiek van signalen, geschriften, beeld, geluid of berichten van welke aard ook, die toegankelijk zijn via toegangsdiensten. Op aanbieders van toegang rust de plicht filterprogrammatuur aan te bieden. De civiele en strafrechtelijke aansprakelijkheid van aanbieders van toegang of opslag wordt beperkt. Een Internet-aanbieder kan namelijk slechts aansprakelijk gesteld worden voor onrechtmatige informatie, wanneer aan een (of meer) van drie voorwaarden is voldaan:

1. de aanbieder heeft bijgedragen aan de schepping of voortbrenging van de inhoud, of hij respecteert de voorwaarden niet die de rechthebbende aan toegang tot de inhoud heeft verbonden, of
2. de aanbieder van opslagdiensten heeft niet prompt de toegang tot een inhoud geblokkeerd, hoewel hij tot blokkering aangemaand was door een rechterlijke autoriteit, of
3. de aanbieder van opslagdiensten heeft niet de gepaste zorgvuldigheid in acht genomen nadat hij in gebreke is gesteld door een derde die van oordeel is dat inhoud die de aanbieder opslaat en aanbiedt onrechtmatig is en hem schade berokkent.

Ondertussen geeft de rechtspraak het volgende beeld van de aansprakelijkheid van Internet-aanbieders onder het huidige recht. Smaad valt onder de wet van 1982 over 'communication audiovisuelle'. Het Tribunal de Grand Instance te Puteaux kwam in de zaak AXA/M. tot het oordeel dat een opslagaanbieder in beginsel niet aansprakelijk is voor van derden afkomstige smaad. Het tribunaal oordeelde namelijk dat (de directeur van) een opslagaanbieder niet is een 'directeur de publication' in de zin van de Franse omroepwet van 1982.[206] Deze wet eist namelijk dat er een vastlegging

204 Zie het commentaar van de senaatscommissie over culturele aangelegenheden, Hugot 1999.
205 De tekst die de Assemblée Nationale op 23 maart 2000 heeft aangenomen is te lezen op <http://www.assemblee-nationale.fr/2/dossiers/communic/2com.htm>.
206 Tribunal de Grand Instance de Puteaux 28 september 1999 (AXA Conseil IARD et AXA Conseil Vie v. M. Christophe M., M. Christophe Sapet, voorzitter van Infonie).

plaatsvindt voorafgaand aan de publicatie.[207] Dat is in de Internet-context niet het geval. Vrijwel op hetzelfde moment dat de informatie wordt geüpload door de inhoudsaanbieder komt deze beschikbaar voor het publiek. Dat snijdt voor de opslagaanbieder iedere mogelijkheid af om enige voorafgaande controle op de inhoud uit te oefenen. De opslagaanbieder is derhalve niet meer dan een dienstverlener die de technische middelen ter beschikking stelt waarmee de inhoudsaanbieder openbaar kan maken.

Waar het gaat om privacyschendingen, meer in het bijzonder schendingen van portretrechten, lijkt de Franse rechter eerder aansprakelijkheid van de opslagaanbieder aan te nemen. Het Tribunal de Grand Instance te Nanterre moest oordelen over de aansprakelijkheid van een viertal Internet-aanbieders die weblocaties aanboden waarop naaktfoto's van een mannequin te zien waren.[208] De publieke beschikbaarstelling van deze afbeeldingen maakte inbreuk op haar portretrechten. De rechter oordeelde dat een opslagaanbieder meer is dan een enkele toegangsverschaffer, omdat hij zich begeeft op het terrein van communicatie van ideeën, meningen, informatie en diensten. Op de opslagaanbieder rust een algemene zorgplicht. Hij moet derhalve de nodige voorzorgsmaatregelen nemen en redelijke middelen inzetten van informatie, waakzaamheid en actie. Deze uitspraak ligt op één lijn met de uitspraken in de zaak Estelle Hallyday/Valentin Lacambre.[209]

Voor de positie van de Internet-aanbieder onder het auteursrecht is een uitspraak van het Tribunal de Commerce te Parijs van belang.[210] Deze uitspraak betrof weliswaar het sui generis-databankrecht, maar gezien de gelijkenis tussen auteursrecht en databankrecht moet kennisname van dit oordeel toch van belang geacht worden voor het auteursrecht. T.I. Communication en M.D. stelden een databank beschikbaar via een weblocatie. Deze beschikbaarstelling maakte inbreuk op de sui generis-databankrechten van Electre. De rechter oordeelde dat op de opslagaanbieder (Maxotex) geen plicht rust om de inhoud te controleren van gegevens waarvan hij de 'omloop' toestaat. Maxotex had overigens prompt na notificatie de inhoudsaanbieder (T.I. Communication) verzocht de gegevens te verwijderen. Toen bleek dat deze daaraan geen gevolg gaf, heeft Maxotex de gegevens zelf verwijderd.

Identificatie van inhoudsaanbieders

De Conseil d'Etat acht blijkens haar rapport *Internet et les réseaux numériques* uit 1998 een versterking van identificatiemogelijkheden van actoren noodzakelijk en ziet verschillende mogelijkheden om dit te realiseren. Hij denkt aan een verplichting voor de uitgever/redacteur van inhoud om eigen identificatie-informatie op te nemen op zijn weblocatie. Voorts zouden toegangsaanbieders nieuwe abonnees om hun identiteit moeten vragen, opdat de toegangsaanbieder in staat is die informatie ingeval van een 'onderzoek' aan politie of justitie te verstrekken. Ten slotte wijst hij op de waarde die door toegangsaanbieders vastgelegde verkeersgegevens vertegenwoordigen voor rechtshandhavers en op het belang dat deze gegevens niet te snel worden gewist. Een verplichting voor toegangsaanbieders om verkeersgegevens een jaar te bewaren – zoals France Telecom doet met betrekking tot gegevens over telefoongesprekken –

---

207 In gelijke zin Cour de Cassation, Chambre Criminelle, 8 december 1998 (Le Procureur général c./M.R.).

208 Tribunal de Grand Instance de Nanterre 8 december 1999 (Lynda Lacoste v. Multimania Company, France Cybermedia Company, SPPI, Estérel Company).

209 Cour d'appel de Paris 10 februari 1999 (Estelle Hallyday/Valentin Lacambre) en Ordonnance de référé – Tribunal de Grande Instance de Paris – 9 juni 1998 (Estelle Hallyday/Valentin et Daniel Lacambre).

210 Tribunal de commerce de Paris 7 mei 1999 (SA Electre v. SARL T.I. Communication, SARL Maxotex Hébergement en M.D.).

komt de Conseil d'Etat echter niet realistisch voor, gezien het feit dat toegangsaanbieders hun gegevens nu veel korter bewaren.[211]

Ook de regering ziet het belang van log-gegevens van Internet-aanbieders voor de rechtshandhaving. Zij zal dan ook in de wet op de informatiemaatschappij preciseren onder welke voorwaarden verkeersgegevens moeten of mogen worden opgeslagen.[212] Bij de beperking van te bewaren gegevens en de begrenzing van de bewaarduur wordt rekening gehouden met drie elementen: de beperkingen van juridische procedures, de kosten die het voor Internet-aanbieders meebrengt en de zorg om ongeoorloofd gebruik van op basis van de wet gevormde bestanden te vermijden.

Inmiddels is in het aanhangige wetsvoorstel tot herziening van wet nr. 86-1067 van 30 september 1986 over de communicatievrijheid via amendementen een uitgebreide regeling over de identificatie van Internet-aanbieders en inhoudsaanbieders opgenomen.[213] Aanbieders van toegang of opslag zijn verplicht gegevens te bewaren die leiden tot identificatie van de persoon die de betreffende inhoud heeft gecreëerd of voortgebracht. De Conseil d'Etat bepaalt de termijn en de modaliteiten van de bewaring van de gegevens. Wanneer een aanbieder daarop wordt aangesproken door een rechterlijke autoriteit, is hij verplicht aan haar de gegevens die hij in zijn bezit heeft over te brengen (art. 43-6-3).

Op online inhoudsaanbieders rust een directe of indirecte identificatieplicht. Zij moeten hun naam, woonplaats en bedrijfsvorm en de naam van de 'directeur de la publication' en zo mogelijk de hoofdredacteur aan het publiek bekendmaken. De plicht geldt niet voor privé-correspondentie. Dienstverleners die niet professioneel optreden kunnen volstaan met het bekendmaken aan het publiek van hun pseudoniem en de naam van de opslagaanbieder. Aan de opslagaanbieder moeten dan weer wel alle bovengenoemde gegevens bekend gemaakt worden. De opslagaanbieder ziet toe op naleving van alle voornoemde identificatieplichten door degenen voor wie hij inhoud opslaat (art. 43-6-4).

Internationale regulering
Nationale regulering van de civiele aansprakelijkheid van intermediairen dient naadloos aan te sluiten bij regulering op Europees en internationaal vlak. Er bestaat een voorkeur voor zelfregulering.[214]

Grensoverschrijdende aspecten
Er bestaan op dit moment geen plannen de bestaande IPR-regels aan te passen, zelfs als het risico toeneemt dat conflicten juridisch aanknopingspunten vertonen met meerdere plaatsen en de moeilijkheden rond de uitvoerbaarheid van jurisprudentiële oplossingen zich verscherpen.[215]

8.5 Verenigd Koninkrijk

Aansprakelijkheid van Internet-aanbieders
Het Verenigd Koninkrijk kent geen algemene regeling voor de aansprakelijkheid van Internet-aanbieders.

---

211 Conseil d'Etat 1998.
212 Strauss Kahn e.a. 1999, p. 33.
213 De tekst die de Assemblee Nationale op 23 maart 2000 heeft aangenomen is te lezen op <http://www.assemblee-nationale.fr/2/dossiers/communic/2com.htm>.
214 G. Chatillon, interview.
215 Conseil d'Etat 1998, par. 4.1.2.

In 1996 is de wetgeving over smaad ingrijpend hervormd door invoering van de Defamation Act (DA) 1996. Deze wet verschaft een 'innocent dissemination'-verweer aan een persoon die niet de auteur, redacteur of uitgever is van de smadelijke uiting (art. 1 lid 1 sub a DA 1996). Zo komt het verweer bijvoorbeeld toe aan de beheerder of toegangsaanbieder van een communicatiesysteem, door middel waarvan een persoon waarover hij geen effectieve controle had de smadelijke uiting heeft getransporteerd of beschikbaar gesteld.[216] Het verweer is beschikbaar, mits aan een tweetal voorwaarden is voldaan. De Internet-aanbieder heeft redelijkerwijze zorgvuldig gehandeld en wist niet en had ook geen reden om aan te nemen dat hij de publicatie van de smadelijke uiting (mede) veroorzaakte of daaraan bijdroeg. Het Crown Court te Leicester heeft in *Godfrey/Demon* inmiddels beslist dat een Internet-aanbieder zich in beginsel op het verweer kan beroepen (dat wil zeggen: hij is niet als auteur enzovoorts aan te merken).[217] In casu is het verweer echter niet gehonoreerd, omdat de Internet-aanbieder onzorgvuldig had gehandeld. Hij had namelijk nagelaten de betreffende smadelijke nieuwsberichten te wissen na notificatie door het slachtoffer. De rechter was van oordeel dat de notificatie wetenschap bij de Internet-aanbieder opleverde.

Aansprakelijkheid van de Internet-aanbieder voor auteursrechtinbreuk wordt beheerst door de gewone regels van auteursrecht (1988 Copyright Designs and Patents Act). De Internet-aanbieder is onder omstandigheden aansprakelijk als bevorderaar van inbreuk (*secondary infringer*). Voor bevordering van inbreuk is wetenschap vereist. Het Trade and Industry Committee van het Lagerhuis is – evenals de regering – voorstander van een goede balans tussen de belangen van rechthebbenden en gebruikers van informatie.[218] Om de rechtsonzekerheid voor Internet-aanbieders weg te nemen moeten, naar de mening van de commissie, de Harmonisatierichtlijn en de Elektronische-handelsrichtlijn zo spoedig mogelijk in de Britse nationale wetgeving worden gä mplementeerd.

Voor aansprakelijkheid voor privacy-inbreuken moet men kijken naar de huidige Interception of Communications Act 1985. Deze heeft alleen betrekking op de post en openbare telecommunicatie systemen en kan slechts gehandhaafd worden met betrekking tot gelicentieerde openbare telecomaanbieders (Public Telecommunications Operators, PTO) en het Post Office. De verzorging van e-post door een Internet-aanbieder wordt niet bestreken door de wet van 1985.[219] De Regulation of Investigatory Powers Bill (hierna: RIP Bill) beoogt hierin verandering te brengen.[220] Het wetsvoorstel voorziet in strafbaarstelling van ongeoorloofde onderschepping van een bericht, gedurende de transmissie ervan via een openbaar of privaat communicatiesysteem. Transmissie omvat mede de tussentijdse opslag in een telecommunicatiesysteem die plaatsvindt om de geadresseerde in staat te stellen de informatie op te halen of er anderszins toegang toe te verkrijgen (art. 2.7 RIP Bill), zoals de opslag in een e-postbus.

Identificatie van inhoudsaanbieders

In 1996 is een convenant tot stand gekomen tussen de Internet Watch Foundation (IWF) – het Engelse Internetmeldpunt – en organisaties van Internet-aanbieders (ISPA en LINX): het Safety Net Agreement. Het is de grondslag voor zelfregulering door Internet-aanbieders in het Verenigd Koninkrijk. Voor aangesloten Internet-

216 Zie art. 1 lid 1 jo. lid 3 sub e Defamation Act 1996. Mogelijk kan een Internet-aanbieder zich ook beroepen op art. 1 lid 1 jo. lid 3 sub c Defamation Act 1996.

217 High Court of Justice, Queen's Bench Division, Hon. mr Justice Morland 26 maart 1999 (Laurence Godfrey/Demon Internet Limited).

218 House of Commons 1999, par. 110.

219 Jabbour 1999, p. 390.

220 Zie <http://www.homeoffice.gov.uk/oicd/ripbill.htm>.

aanbieders vestigt het onder andere verplichtingen over identificeerbaarheid en traceerbaarheid van Internetgebruikers. Internet-aanbieders moeten samenwerken met de IWF teneinde verschaffers van onrechtmatig materiaal te identificeren, zij moeten nieuwe maatregelen onderzoeken tegen identificatie-gaten, en zij moeten betere traceerbaarheid faciliteren, bijvoorbeeld door verschaffing van *audit-trails* en maatregelen ter verbetering van de identificeerbaarheid van gebruikers van 'gratis' Internet.[221]

Verstrekking van identificatie-informatie door Internet-aanbieders aan slachtoffers wordt geregeerd door de Data Protection Act 1998 of vindt plaats in het kader van de waarheidsvinding tijdens gerechtelijke procedures.[222]

Internationale regulering
De regering onderschrijft het Europese actieplan over veilig gebruik van Internet, waarin internationale samenwerking en zelfregulering de sleutelwoorden zijn. Onder andere wordt gesproken over een Europees netwerk van meldpunten.[223]

Grensoverschrijdende aspecten
De IWF geeft meldingen over kinderpornografie die op een buitenlandse server staat door aan de NCIS (UK National Criminal Intelligence Service), die de melding op zijn beurt weer doorspeelt aan Interpol of rechtstreeks aan de betreffende buitenlandse politie-autoriteiten. De IWF leidt meldingen over andere onrechtmatige inhoud die op een buitenlandse server staat niet door. Uit het evaluatierapport over het functioneren van de IWF blijkt dat de NCIS een achterstand heeft met het doorsturen van (kinderpornografie-)meldingen naar Interpol en buitenlandse politie-autoriteiten.[224]

8.6 Verenigde Staten

Aansprakelijkheid van Internet-aanbieders
De regering van de VS is geen voorstander van regulering van Internet-inhoud zelf. Slechts als het gaat om voorkoming van fraude, acht zij overheidsbemoeienis op zijn plaats.[225] De Verenigde Staten kennen aparte regelingen over de aansprakelijkheid van Internet-aanbieders. Anders dan Duitsland of de Europese Unie hebben de VS niet gekozen voor een horizontale benadering.

De Digital Millennium Copyright Act (hierna: DCMA) voorziet in een *notice-and-take-down*-regime. Rechthebbenden die een onrechtmatige beschikbaarstelling van hun werk op het Internet aantreffen, kunnen de Internet-aanbieder een kennisgeving sturen. Indien de kennisgeving aan bepaalde formele eisen voldoet moet de Internet-aanbieder de informatie ontoegankelijk maken en de kennisgeving aan de inhoudsaanbieder doorspelen. Deze kan binnen een bepaalde termijn een tegenmelding (*counter-notice*) uitbrengen. De rechthebbende is dan weer aan zet. Doet hij niets dan zal de Internet-aanbieder de informatie na het verstrijken van een termijn weer toegankelijk maken. De rechthebbende kan dit slechts voorkomen door binnen de termijn de zaak aanhangig te maken bij de rechter. Het moge duidelijk zijn dat de

221 Art. 30 Safety Net Agreement, zie <http://www.iwf.org.uk/about/R3Safety.html>.
222 In *E-commerce@its.best.uk* wordt een aanbeveling gedaan die van belang kan worden voor identificatie van inhoudsaanbieders: de regering wil het gebruik van multifunctionele smartkaarten bevorderen, waarbij men aan een ruim toepassingsbereik denkt. Dit omvat onder andere identificatie-functies. Smartkaartlezers zouden in de toekomst standaard in pc's ingebouwd moeten worden. Cabinet Office 1999, aanbeveling 10.3.
223 Battle 1998, p. 8.
224 KPMG & Denton Hall 1999, par. 4.1.2.2 .
225 White House 1997, p. 25-26.

Internet-aanbieder die aan de zorgvuldigheidsverplichtingen van de DCMA voldoet niet aansprakelijk is. In de rechtspraak van voor inwerkingtreding van de DCMA wordt de Internet-aanbieder aangemerkt als medeplichtige (*contributory infringer*). Hiervoor is wel wetenschap vereist.[226]

De Communications Decency Act[227] bevrijdt Internet-aanbieders vergaand van aansprakelijkheid voor smadelijke uitlatingen afkomstig van derden: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (47 USC 230 (c) (1)). Dit privilege is beschikbaar voor de Internet-aanbieder onafhankelijk van zijn wetenschap. De achtergrond hiervan is dat het Congres een *chilling effect* op de vrijheid van meningsuiting vreesde, indien Internet-aanbieders zich gedwongen zouden zien om de inhoud die zij aanbieden of doorgeven te controleren.[228] Dat dit gevaar niet denkbeeldig is blijkt uit de bekende zaak *Stratton Oakmont/Prodigy*.[229] Tevens zou van deze regeling een stimulans uitgaan op zelfregulering, het zogenaamde *Good Samitaran blocking and screening.* Aansprakelijkheid op basis van wetenschap zou Internet-aanbieders namelijk slechts aanzetten om zich zo afzijdig mogelijk te houden. In dit verband wordt wel gewezen op de andere bekende zaak, *Cubby/CompuServe*.[230]

Identificatie van inhoudsaanbieders

Het *notice-and-take-down*-regime van de DMCA voorziet in de mogelijkheid dat de rechthebbende de griffier van een District Court verzoekt een dwangbevel (*subpoena*) tegen een Internet-aanbieder te verlenen tot identificatie van een vermeende inbreukmaker. Dit dwangbevel wordt verleend indien – eenvoudig gezegd – een deugdelijke notificatie van de betreffende Internet-aanbieder heeft plaatsgevonden. Het dwangbevel houdt in dat de Internet-aanbieder informatie geeft die voldoende is om de vermeende inbreukmaker te identificeren, indien en voorzover de Internet-aanbieder over die informatie beschikt.

Er is een wetsvoorstel aanhangig voor de Consumer Internet Privacy Protection Act of 1999. Deze wet verbiedt – als hij eenmaal van kracht is – dat interactieve computerdiensten identificeerbare persoonsinformatie die afkomstig is van een abonnee zonder diens schriftelijke toestemming (*informed consent*) verstrekken aan enige derde.

Internationale regulering en grensoverschrijdende aspecten

De regering ontwikkelt een informele dialoog met de belangrijkste handelspartners over inhoudskwesties om zeker te stellen dat nationale regulering, met name indien die de strekking heeft de culturele identiteit te behouden, niet functioneert als een vermomde handelsbelemmering.[231] Tevens zoekt zij in dialoog met andere landen naar

---

226 Zie onder andere Sega Entertainment Ltd./Maphia, no. C93-04262 (N.D. Cal. 1996) en Religious Technology Center v. Netcom Online Communications Services, 907 F. Supp. 1361 (N.D. Cal. 1995).

227 Het gaat hier niet om de bepaling uit de CDA die door het hooggerechtshof ongrondwettig is verklaard.

228 Dit blijkt bijvoorbeeld uit U.S. 4th Circuit Court of Appeals 12 november 1997 (Zeran v. America Online Inc.). Zie ook John Doe v. America Online, Case No. 97-2587, 718 So. 2d 385; 1998 Fla. App. LEXIS 1248.

229 Stratton Oakmont v. Prodigy Services Co., No.31063/94, 1995 WL 323710 (N.Y. Sup. Court May 1995). De rechter oordeelde dat Prodigy aansprakelijk was voor beledigende inhoud van een derde, waarbij een belangrijke rol heeft gespeeld dat Prodigy enige controle uitoefende op de informatie die zij aanbood.

230 Cubby v. CompuServe, 776 F. Supp. 135 (S.D.N.Y. 1991). De rechter oordeelde dat CompuServe niet aansprakelijk was voor de inhoud van derden, waarbij een rol speelde dat CompuServe alle inhoudelijke bemoeienis had uitbesteed aan een ander bedrijf.

231 White House 1997, p. 26.

manieren om de diversiteit van informatie die op Internet beschikbaar is te bevorderen, zonder de beschikbaarstelling ervan te beperken.

8.7 Andere landen

8.7.1 Australië

Van Australië wordt hier de Broadcasting Services Amendment (On-line Services) Bill 1999 behandeld, omdat deze wet (ook) bepalingen bevat over inhoud die buiten Australië wordt aangeboden. De wet belast de Australian Broadcasting Authority (hierna: ABA) met de taak om hetzij op eigen initiatief, hetzij naar aanleiding van klachten Internet-inhoud te laten classificeren (*rating*) door de Classification Board. Afhankelijk van de uitkomst van een classificatie wordt inhoud beschouwd als verboden (*prohibited*). Inhoud krijgt dit predikaat, indien de Classification Board er de classificatie X (*explicit sexuality*) of RC (*Refused Classification*) aan heeft gegeven (materiaal buiten Australië krijgt overigens geen R-classificatie). Inhoud wordt eveneens als verboden aangemerkt, indien zij als R (*Nudity*) is geclassificeerd en niet onderworpen is aan een 'restricted access system'. Staat verboden materiaal op een server in Australië, dan krijgt de opslagaanbieder een bevel tot verwijdering (*take-down notice*) van de ABA. Hij moet daaraan binnen een werkdag gevolg geven. Tevens moet hij ervoor zorgen dat het materiaal niet meer terugkeert op zijn server. Wordt het materiaal daarentegen buiten Australië aangeboden, dan krijgt de Australische dienstaanbieder die de toegang verzorgde een kennisgeving waarin van hem geëist wordt dat hij alle redelijke stappen onderneemt om toegang tot de inhoud te blokkeren of dat hij de toegang blokkeert overeenkomstig de regels die een (bedrijfsleven)code daarover geeft. Behalve de nakoming van kennisgevingen dient een Internet-aanbieder een groot aantal in codes vast te leggen informatieplichten en procedures na te leven. De wet kent zware sancties (boetes van maximaal A$ 27.500,- per dag!).

De wet heeft veel kritiek gekregen, niet alleen van de Internet-bedrijfstak. De kritiek richt zich op het feit dat de wet alleen aansprakelijkheid voor Internet-aanbieders vestigt en zich niet richt op de inhoudsaanbieder. Zij zou daarmee de kosten van handhaving bij de verkeerde schakel in de distributieketen leggen en migratie van inhoud naar het buitenland in de hand werken. De wet trad in de zomer van 1999 in werking, maar de wet zelf bepaalde dat hij pas effectief zou worden op 1 januari 2000. Voor die datum, op 30 september 1999, heeft de Australische senaat een motie aangenomen waarin zij de regering oproept tegemoet te komen aan de zorgen die bij het bedrijfsleven en het publiek leven over de onwerkbaarheid van de door de regering gekozen benadering en de wet. Tevens wordt de regering gevraagd de ernstigste knelpunten voor 1 januari 2000 weg te nemen. De motie is mede ingegeven door het negatieve effect dat de wet – naar verwachting – heeft op de ontwikkeling van e-handel en de Internet-bedrijfstak in Australië.[232]

8.7.2 Singapore

De Electronic Transactions Act 1998 voorziet in een geclausuleerde vrijstelling van aansprakelijkheid voor toegangsaanbieders voor inhoud van derden (art. 10). Internet-aanbieders moeten zich echter wel laten registreren bij de Singapore Broadcasting Authority en zij moeten op aanwijzing van de SBA de toegang blokkeren tot

[232] Scott 1999, p. 21.

'verwerpelijke' weblocaties. De Singapore Broadcasting Authority (Class Licence) Notification 1996 onderscheidt brede categorieën inhoud die niet onder ogen mogen komen van inwoners van Singapore. Ze hebben betrekking op de algemene veiligheid en nationale defensie, op raciale en religieuze harmonie, op de publieke moraal en op bepaalde overige inhoud. Dit alles heeft niet alleen betrekking op inhoud die in Singapore wordt aangeboden, maar tevens op materiaal van buiten. Het grensoverschrijdend Internetverkeer verloopt via een beperkt aantal proxy-servers waar filtering op inhoud plaatsvindt.[233]

8.7.3 Zweden

Zweden kent sinds 1998 een wet over de verantwoordelijkheid voor Elektronische Bulletin Boards.[234] Algemeen wordt aangenomen dat deze wet eveneens van toepassing is op Internet-aanbieders.[235] Op grond van art. 4 van de wet dient de Bulletin Board-aanbieder controles uit te voeren die redelijkerwijze passen bij de omvang en de aard van de te controleren dienst. Uit de wetsgeschiedenis is af te leiden dat een aanbieder niet ieder bericht hoeft te controleren.[236] Hij kan echter niet langere tijd iedere controle achterwege laten. Hoe vaak hij moet controleren is afhankelijk van de inhoud van de dienst. Commerciële aanbieders moeten intensiever controleren dan privé-diensten. Indien controles – door hun aantal – te belastend worden voor een aanbieder, kan hij aan zijn plicht voldoen door een meldpunt voor onrechtmatige inhoud in te stellen. Kennelijk onrechtmatige berichten dient de aanbieder te verwijderen.[237] Teneinde aan deze plicht te kunnen voldoen, heeft de aanbieder de bevoegdheid de inhoud van berichten te inspecteren. Mogelijk strekt deze controlebevoegdheid zich ook uit over gesloten gebruikersgroepen. Het niet voldoen aan de verwijderplicht is strafrechtelijk gesanctioneerd.

8.8 Vergelijking en conclusie

De materiële criteria die in de verschillende landen worden aangelegd voor aansprakelijkheid van Internet-aanbieders (zoals inhoudelijke betrokkenheid, wetenschap en zorgvuldigheid) vertonen gelijkenis. In de eerste plaats valt op dat in de onderzochte landen onderscheid wordt gemaakt tussen actoren die inhoudelijk betrokken zijn bij een informatie-aanbod en degenen die slechts materieel steun verlenen aan de verspreiding van informatie door derden.[238] De eersten zijn volledig verantwoordelijk voor de inhoud, de laatsten zijn slechts aansprakelijk indien zij zorgvuldigheidsnormen overtreden. In Nederland wordt dit onderscheid zowel in de wetgeving [239] als in de rechtspraak onderschreven. In sommige landen wordt binnen de categorie van materiële steunverleners nog onderscheid gemaakt tussen aanbieders die slechts toegangsdiensten verlenen en anderen die opslagdiensten aanbieden (bijvoorbeeld in Duitsland art. 5 TDG en in de EU art. 12 en 14 Elektronische

233 Hogan 1999.

234 Lag (1998:112) om ansvar för elektroniska anslagstavlor.

235 Palme 1998.

236 Palme 1998.

237 De verwijderingsplicht geldt niet voor iedere onrechtmatige inhoud, maar slechts voor de in art. 5 genoemde delicten: opruiing, aanzetten tot raciale haat, kinderpornografie, verheerlijking van geweld en auteursrechtinbreuk.

238 Enkele voorbeelden: in Duitsland art. 5 TDG, in Frankrijk voorstel voor art. 43-6-2.II (eerste gedachtestreepje) Wet van 30 september 1986 over de communicatievrijheid, in het Verenigd Koninkrijk art. 1 lid 1 sub a Defamation Act 1996 en in de Verenigde Staten 47 USC 230 sub c.

239 De aanvankelijk in het wetsvoorstel Computercriminaliteit II voorgestelde niet-vervolgbaarheid was slechts beschikbaar voor de 'tussenpersoon als zodanig'.

handelsrichtlijn). In Nederland is het aan de rechter om rekening te houden met de aard van de activiteiten (toegang of opslag), indien dit van belang is voor het oordeel over de zorgvuldigheid die een aanbieder heeft betracht.[240] Zo overwoog de president van de Haagse rechtbank in het Scientology-vonnis over Internet-aanbieders: "Zij verschaffen slechts de technische faciliteiten teneinde openbaarmaking door anderen mogelijk te maken". [241]

In de onderzochte landen is een – als materieel steunverlener optredende – dienstaanbieder slechts aansprakelijk voor onrechtmatige inhoud waarvan hij daadwerkelijk op de hoogte is. Van dit uitgangspunt wordt afgeweken in twee richtingen. Enerzijds kent Zweden bijvoorbeeld een pro-actieve controleplicht voor dienstaanbieders.[242] Gezien het feit dat een aanbieder door het oprichten van een meldpunt aan deze verplichting kan voldoen, kan echter gesteld worden dat ook in Zweden geen resultaatsverplichting op dienstaanbieders wordt gelegd om hun systeem 'schoon' te houden. Anderzijds zijn er regelingen (in Duitsland en de EU) waarin de toegangsverschaffer een aparte positie heeft, in die zin dat hij niet aansprakelijk is, ongeacht wetenschap. In de praktijk zullen toegangsaanbieders overigens vaak geen 'wetenschap' hebben, noch in staat zijn op te treden tegen inhoud. In Nederland is 'daadwerkelijke wetenschap' net als in de meeste landen een onrechtmatigheid-constituerende factor (zie het hierboven genoemde Scientology-vonnis), ook bij toegangsaanbieders. Wanneer de Europese Richtlijn van kracht wordt, zal Nederland op dit punt het standpunt moeten aanpassen. Onder de inmiddels ingetrokken regeling die het wetsvoorstel Computercriminaliteit II voor tussenpersonen trof, hoefden tussenpersonen pas in te grijpen, indien zij daartoe door de Officier van Justitie waren aangemaand; enkel wetenschap verplichtte de tussenpersoon niet tot ingrijpen.[243] Dit kan verklaard worden uit de bijzondere ratio van deze regeling: het voorkomen van 'censuur' door tussenpersonen.

Ten slotte rust in alle landen op een dienstaanbieder de zorgplicht om (bij daadwerkelijke wetenschap) onrechtmatige informatie weg te halen of de toegang ertoe te blokkeren, voorzover hij daartoe redelijkerwijze in staat is.

In de onderzochte landen lijkt men in te zien dat Internet-aanbieders een bijzondere rol en verantwoordelijkheid hebben in de identificatie van inhoudsaanbieders. De verantwoordelijkheid hoeft niet slechts te bestaan uit het desgevraagd verstrekken van identificatiegegevens waarover de aanbieder beschikt, maar het kan ook gaan om voorbereidende maatregelen om aan een toekomstige identificatie-vraag te kunnen voldoen, zoals bewaring van gegevens en verificatie van de identiteit van nieuwe abonnees. De wijze waarop bij de afbakening en vormgeving van deze verantwoordelijkheden recht kan worden gedaan aan privacy-belangen baart de meeste landen echter nog kopzorgen. Frankrijk gaat vooralsnog voorop in identificatie-regulering. Er is een wetsvoorstel aanhangig dat plichten op aanbieders legt die betrekking hebben op het beschikbaar stellen, bewaren en verstrekken van (verkeers)gegevens. Het Nederlandse standpunt strookt al met al met ontwikkelingen die in het buitenland ontwaard kunnen worden.

---

240 Vergelijk TK 1998-1999, 25880, nr. 7, p. 4. In Nederland wordt de voorkeur gegeven aan rechtsontwikkeling door de rechter.

241 R.o. 16 in Pres.Rb. 's-Gravenhage 9 juni 1999, *Informatierecht/AMI* 1999, p. 100 e.v. (Scientology/Xs4all).

242 In Franse rechtspraak over inbreuk op portretrechten wordt ook wel een monitorverplichting aangenomen.

243 Opzet op de aard van de inhoud is wel van belang voor kwalificatie onder art. 418 Sr: de strafbaarstelling van het niet voldoen aan de zorgvuldigheidsplichten van art. 53 Sr. Bovendien is 'wetenschap' van belang indien een dienstaanbieder geen beroep kan doen op de niet-vervolgbaarheid van art. 53 Sr; hij is dan aansprakelijk volgens de gewone regels van strafrecht.

De algemene houding met betrekking tot grensoverschrijdende aspecten wordt vooral door terughoudendheid gekenmerkt. Aansprakelijkheid van toegangsaanbieders wordt niet gezien als een middel om greep te krijgen op de binnenlandse beschikbaarheid van onrechtmatige inhoud die in het buitenland wordt aangeboden. Australië en Singapore moeten in dit opzicht als uitzonderingen op de regel worden gezien.

Nationale overheden beschikken over voldoende handelingsvermogen met betrekking tot Internet-aanbieders die zich op hun grondgebied bevinden om hun aansprakelijkheid op een effectieve manier te regelen. Vanuit het perspectief van het nationale handelingsvermogen is er derhalve geen reden dit op internationaal niveau te regelen. De regeling in de Europese Elektronische handelsrichtlijn dient vooral om divergentie tussen nationale wetgeving en rechtspraak te voorkomen dan wel te beperken.[244]

Voor het internationale probleem van schadelijke en illegale inhoud – de aanpak van in een land verkrijgbare onrechtmatige inhoud die vanuit het buitenland wordt aangeboden – zijn evenwel geen oplossingen voorhanden. Een vergaande harmonisatie van materiële normen lijkt nauwelijks te bereiken. Men beperkt zich vooralsnog tot de internationale samenwerking van meldpunten.

[244] Zie overweging 40 van (het gemeenschappelijk standpunt van de Raad van 28 februari 2000 met betrekkeing tot) de Richtlijn inzake elektronische handel.

9. Samenvatting en conclusies

9.1 Inleiding

Uit de in de voorgaande hoofdstukken gepresenteerde resultaten van het rechtsvergelijkend onderzoek naar internationalisering en rechtsmacht in Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten vallen diverse conclusies te trekken. In het onderstaande presenteren we allereerst een samenvatting aan de hand van de in dit rapport gehanteerde tweedeling tussen algemene thema's (par. 9.2) en specifieke onderwerpen (par. 9.3).[245] Vervolgens trekken we conclusies en plaatsen we kanttekeningen op basis van enkele afwegingen en onderscheidingen die relevant zijn voor een standpunt inzake regulering van de elektronische snelweg (par. 9.4). Ten slotte formuleren we op basis van al deze conclusies een centrale eindconclusie van dit onderzoek (par. 9.5).

9.2 Algemene thema's

Wat allereerst opvalt bij het rechtsvergelijkend onderzoek naar standpunten inzake regulering van de elektronische snelweg, is dat er weinig alomvattende juridische beleidsdocumenten zoals *Wetgeving voor de elektronische snelweg* zijn; alleen Frankrijk heeft een soortgelijke poging gedaan met het consultatiedocument *Une société de l information pour tous*, dat een opmaat beoogt te zijn voor een breed wetsvoorstel. De overige landen beperken zich tot beleidsdocumenten over bijvoorbeeld elektronische handel of nog specifiekere onderwerpen als belastingen of illegale en schadelijke inhoud.

Niettemin komen in grote lijnen de visies van de onderzochte landen op de aanpak van ICT-recht in het licht van internationalisering en rechtsmacht overeen. Dit geldt allereerst voor het in de nota WES gehanteerde uitgangspunt dat wat offline geldt, ook online moet gelden. Hoewel alleen het VK (evenals Australië) expliciet ook dit uitgangspunt heeft erkend, valt uit de beleids- en wetgevingsinitiatieven in de andere landen af te leiden dat ook zij dit uitgangspunt in grote lijnen hanteren. Toch bestaat er in toenemende mate ruimte voor afwijking daarvan, omdat blijkt dat voor het veiligstellen van de achterliggende belangen soms andere regels nodig zijn. Het gaat daarbij overigens zowel om rechtsstatelijke belangen (zoals fundamentele normen en waarden en consumentenbescherming) als om economische belangen. Het uitgangspunt kan dan ook beter genuanceerd worden zoals de VS dat heeft uitgesproken: het beschermingsniveau in de online wereld moet hetzelfde zijn als dat in de offline wereld. Anders gezegd: voor regelgeving op de elektronische snelweg moet men veel meer kijken naar de achterliggende belangen dan naar de specifieke

[245] We vatten hier het rapport op hoofdlijnen samen en herhalen niet alle conclusies uit de verschillende hoofdstukken. Zie daarvoor de *Summary*.

concretisering daarvan in de huidige wet- en regelgeving. Overigens lijkt ook de waarde van het adagium af te nemen naarmate het ICT-recht zich verder ontwikkelt: in plaats van het transponeren van offline regels of belangen naar online regels en belangen, zou het beleid veeleer moeten uitgaan van de eigenheid van de online problematiek.

Opvallend is wel dat het uitgangspunt vooral op nationaal niveau speelt. Voor de internationale aanpak van ICT-recht stelt alleen het VK dat in internationale onderhandelingen ook dit uitgangspunt moet worden gehanteerd. Dit heeft tot gevolg dat de succeskans van internationale samenwerking en harmonisatie, waarvan alle landen de noodzaak onderkennen, in belangrijke mate zal afhangen van de mate van overeenstemming van de achterliggende nationale belangen.

Vergelijkbare visies zijn ook te vinden waar het de rol van zelfregulering betreft. Daarbij valt overigens wel een ontwikkeling waar te nemen van voorrang voor pure zelfregulering naar een meer sturende rol voor de overheid (co-regulering). Zo moet de overheid kaders scheppen voor elektronische handel en schadelijke en illegale inhoud. Deze ontwikkeling wordt ingegeven door strategische redenen (zoals de noodzaak van een integrale aanpak – pure zelfregulering leidt te veel tot ad-hoc-initiatieven, en om door een duidelijk ICT-rechtkader de concurrentiepositie te verstevigen) en door inhoudelijke redenen, zoals rechtszekerheid en de bescherming van de culturele identiteit. Ook leidt de noodzaak van handhaving, die in alle landen breed wordt erkend, tot een grotere rol van de overheid – zelfregulering is geen adequaat instrument om naleving te waarborgen.

Toch zijn er wel verschillen te onderkennen in de status van zelfregulering of co-regulering. In Duitsland, het VK en de VS staat zelfregulering voorop, waarbij de overheid een dialoogpartner is, terwijl in Frankrijk overheidsregulering voorop blijft staan, waarbij zelfregulering een aanvullende rol speelt. Daarbij komt dat vooralsnog onduidelijk is wat precies onder co-regulering verstaan dient te worden: de invulling blijkt in belangrijke mate afhankelijk van de wetgevings- en de culturele traditie van een land.

Het laatste in deze studie behandelde algemene thema uit de nota WES, hoe de handhaving te waarborgen, komt in de officiële documenten van de onderzochte landen minder duidelijk naar voren. Hoewel er veel wordt nagedacht over de noodzaak en de mogelijkheden om handhaving van ICT-recht in de internationale context te waarborgen, zwijgen de overheden vooralsnog over een integrale benadering van handhaving. Men kijkt van geval tot geval wat de beste aanpak is, hetgeen overeenkomt met de pragmatische benadering van Nederland in dezen. Opvallend is daarbij ook dat bij de onderwerpen die algemeen als potentieel moeilijk handhaafbaar in een internationale context worden beschouwd, zoals belasting, privacy en cryptografie, er weinig concrete ideeën bestaan hoe deze op internationaal niveau aangepakt zouden moeten worden.

Daar waar de te waarborgen belangen internationaal breed worden gedeeld, zal de meeste kans bestaan op een internationale aanpak van de problemen. Op de workshop werd gesteld dat het raadzaam is te beginnen op kleine terreinen waar meer overeenstemming bestaat, zoals bij de bestrijding van kinderporno, waarvoor al een internationaal netwerk van meldpunten actief is. Constructies met nationale contactpunten zijn op korte termijn het meestbelovend om handhaving internationaal aan te pakken. Op privaatrechtelijk gebied kan men denken aan een internationaal netwerk van ombudsmensen of Kamers van Koophandel die een centrale rol kunnen spelen bij internationale alternatieve geschillenbeslechting. Binnen het strafrecht concentreert men zich vooralsnog op een internationaal netwerk van nationale contactpunten die 24 uur per dag en zeven dagen per week bereikbaar zijn om direct verzoeken om wederzijdse rechtshulp af te handelen en te coördineren. Dit netwerk

kan een aanzet vormen voor verdergaande vormen van grensoverschrijdende samenwerking.

Concluderend constateren we dat de algemene uitgangspunten uit de nota WES weliswaar in grote lijnen gedeeld worden in de onderzochte landen, maar dat er tegelijkertijd een ontwikkeling gaande is die noopt tot nuancering van de algemene uitgangspunten. Waar concrete onderwerpen geregeld moeten worden, blijken de uitgangspunten niet altijd zo eenvoudig toepasbaar. De algemene adagia zijn wat dat betreft mooie uitgangspunten, maar naarmate het ICT-recht meer tot wasdom komt, blijkt de wereld toch genuanceerder in elkaar te zitten.

9.3 Specifieke onderwerpen

Wat betreft het *strafrecht* zijn binnen dit onderzoek de onderwerpen dubbele strafbaarheid en samenwerking van handhavingsautoriteiten onderzocht.

We stellen vast dat het idee van de Nederlandse regering om in bepaalde gevallen de dubbele strafbaarheid los te laten, in het buitenland nauwelijks weerklank vindt. Bij de voorbereiding van het verdrag *Crime in Cyberspace* binnen de Raad van Europa is er wel over gediscussieerd, maar het ontwerpverdrag laat het vereiste alleen los voor het geven van een rechtshulpverzoek voor een bevel tot *bewaring* van gegevens bij een buitenlandse Internet-aanbieder (hierover is overigens nog geen overeenstemming bereikt: bepaalde staten behouden zich het recht voor het vereiste hier te handhaven). Maar een bewaringsbevel zal de verzoekende staat niet baten als het vereiste vervolgens blijft bestaan voor het kunnen *inzien* van de gegevens, en de ontwerptekst stelt niet ter discussie dat staten bij dit laatste dubbele strafbaarheid kunnen eisen. De verzoekende staat vindt daarom in het verdrag geen effectief middel om gegevens (bijvoorbeeld ter tracering van een digitaal spoor) te verkrijgen als het onderzochte feit in de andere staat niet strafbaar is. De internationale workshop leidde ook tot de conclusie dat het vrijwel onmogelijk is om aan het beginsel van dubbele strafbaarheid te tornen. De landen hechten te zeer aan de nationale soevereiniteit.

Het vasthouden aan nationale soevereiniteit en nationale belangen bij strafrecht betekent dat op internationaal niveau harmonisatie en samenwerking het maximaal haalbare zijn. Zelfs harmonisatie is uiterst moeilijk te bewerkstelligen, gezien de verscheidenheid van achterliggende culturele belangen. Daarom zal het oplossen van problemen op gebied van internationalisering en strafrecht vooral neerkomen op samenwerking tussen handhavingsautoriteiten (waarbij men zich overigens moet realiseren dat verschillen in materiële normen door het vereiste van dubbele strafbaarheid ook invloed hebben op de strafvorderlijke bevoegdheden). Hier zien we verscheidene internationale initiatieven, waarbij de ogen vooral gericht zijn op het toekomstige verdrag *Crime in Cyberspace*. In grote lijnen zijn de landen het wel eens over de onderwerpen en de hoofdlijnen van de regeling, maar het ontwerpen van het verdrag gaat langzaam en heeft tot nu toe ook grotendeels buiten de publiciteit en de publieke oordeelsvorming plaatsgevonden – pas in april 2000 werd een eerste tekst gepubliceerd. We kunnen dan ook concluderen dat beleid en regelgeving van strafrechtelijke onderwerpen in het licht van internationalisering en rechtsmacht moeilijk tot stand zal komen. De enige mogelijkheid om op dit vlak iets tot stand te brengen is te beginnen bij onderwerpen waarover internationaal een aanzienlijke mate van overeenstemming bestaat, met name daar waar de achterliggende belangen gedeeld worden, zoals in de financiële sector. Langzaamaan kunnen dan stukje bij beetje de moeilijker onderwerpen, waar minder overeenstemming over bestaat, ter hand worden genomen.

Ten aanzien van de *privaatrechtelijke* onderwerpen is onderzoek gedaan naar toepasselijk recht bij online overeenkomsten en aansprakelijkheid van Internet-aanbieders. Daarnaast werd op de internationale workshop ook veel aandacht besteed aan elektronische handtekeningen.

Het vraagstuk van toepasselijk recht bij online overeenkomsten is een onderwerp dat niet op het niveau van nationale overheden speelt maar dat bij uitstek binnen internationale organisaties moet worden besproken, zoals binnen de EU en mondiaal binnen het verband van de Haagse Conferentie voor ipr. De Europese ontwerp-Richtlijn Elektronische Handel voorzag aanvankelijk wel in een regeling op dit vlak, maar stelt inmiddels niet tot doel te hebben om specifieke ipr-verwijzingsregels binnen de E-handelrichtlijn te geven. De Commissie besloot het onderwerp van het toepasselijk recht voor wat betreft consumentenrelaties buiten het kader van de Richtlijn Elektronische Handel te laten. Voor *business-to-business* online transacties geldt conform deze Richtlijn het principe van het land van oorsprong. Verder blijkt de door de Nederlandse regering voorgestane aanpassing van de Haagse Conferentie niet spoedig te verlopen. Tijdens een bijeenkomst eind februari 2000 te Ottawa bleek een overeenstemming over het voorliggende concept voor een wijziging van de huidige tekst van de Conferentie verre van haalbaar. Nederland blijkt ten aanzien van het recht dat van toepassing is op online overeenkomsten overigens meer oog te hebben voor een mondiale aanpak dan de onderzochte landen.

De aansprakelijkheid van Internet-aanbieders is een onderwerp dat in alle landen een topactualiteit is. Het beleid op dit gebied heeft in alle landen door wetgeving en jurisprudentie al vorm gekregen, waarbij blijkt dat de gehanteerde materiële criteria in alle landen grotendeels gelijk zijn. Hoewel Zweden en Duitsland op een enkel onderdeel een afwijkende regeling kennen, komt de civiele aansprakelijkheidspositie van de Internet-aanbieder in de praktijk overal op hetzelfde neer. De regeling van aansprakelijkheid van Internet-aanbieders biedt aldus een oplossing voor inbreukmakende inhoud op het Internet. Daarbij valt echter op dat het vooralsnog alleen een oplossing vormt voor inbreukmakende inhoud die *nationaal* wordt aangeboden; de landen zijn uiterst terughoudend bij het aansprakelijk stellen van nationale aanbieders voor buitenlandse inhoud. Daarmee wordt het internationale probleem van schadelijke en illegale inhoud dus niet opgelost. Er zijn vooralsnog geen initiatieven om dat probleem internationaal aan te pakken, anders dan het marktinitiatief van meldpunten, die inmiddels ook internationaal samenwerken.

Binnen het privaatrecht valt verder op dat het algemene beleid van voorkeur voor zelfregulering bepaald niet overal tot afzien van wetgeving heeft geleid. Dit valt met name af te lezen aan de stortvloed van wetgeving op het gebied van de elektronische handtekening (alleen al in de VS zijn hierover 252 wetten in 50 staten gelanceerd). De reden hiervoor is dat dit onderwerp een vraagstuk is van rechtszekerheid: de markt wil een concreet antwoord op de vraag of e-handtekeningen rechtsgeldig zijn. Op nationaal niveau (en binnen federale staten op staatniveau) beoogt wetgeving een antwoord te geven, terwijl tegelijkertijd op internationaal niveau (binnen de EU en UNCITRAL) afstemming tussen de nationale wetgevingen plaatsvindt. De benadering van onderaf en bovenaf heeft vooralsnog niet tot eenduidige regelgeving geleid, maar het is zeker mogelijk dat de initiatieven convergeren naar een internationaal afgestemd beleid.

Een dergelijke convergentie is moeilijker voorstelbaar bij onderwerpen die niet alleen om antwoorden vragen, maar ook om sturing, zoals bij privacy. Marktpartijen accepteren namelijk veel sneller wetgeving die primair antwoorden geeft dan wetgeving die ook hun gedrag poogt te bä nvloeden. Dit verklaart mede de slepende strijd tussen de EU en de VS op het gebied van privacy. De wetgevingstradities die samenhangen met verschillende visies op de manier waarop aan sturing vorm kan worden gegeven, betekenen dat overeenstemming tussen de EU en de VS op dit

terrein moeilijker tot stand kan komen dan bij onderwerpen die voornamelijk om 'antwoorden' vragen, zoals elektronische handtekeningen.

9.4 Afwegingen en onderscheidingen

Een blik op de individuele conclusies laat zien dat diverse afwegingen en onderscheidingen een rol spelen bij het formuleren van beleid voor de elektronische snelweg. We doelen daarbij op een afweging zoals die tussen overheidsregulering enerzijds en marktregulering anderzijds en een onderscheid tussen het beantwoorden van vragen en het sturen van gedrag. We presenteren de resultaten van het onderzoek hier aan de hand van deze en andere dichotomieën, waarbij we zullen ingaan op de implicaties voor het thema rechtsmacht en internationalisering. Overigens zullen we vanuit de insteek van de dichotomie ook de nuances van de onderscheidingen en afwegingen belichten.

9.4.1 Offline – online

Recentelijk valt in alle onderzochte landen een duidelijke ontwikkeling te signaleren die noopt tot nuancering van het in het verleden gehanteerde algemene uitgangspunt "wat offline geldt dient ook online te gelden". Waar momenteel concrete onderwerpen geregeld moeten worden, blijkt dit enkele jaren geleden gä ntroduceerde adagium niet altijd eenvoudig toepasbaar. Het lijkt een waardevol uitgangspunt te zijn geweest voor het embryonale stadium van ICT-regulering, maar naarmate het ICT-recht meer tot wasdom komt, blijkt de wereld toch genuanceerder in elkaar te zitten. Aandacht voor de belangen achter de concrete regels is daarbij op zijn plaats.

Voor het thema rechtsmacht en internationalisering betekent dit dat die factoren die de achter de regels liggende belangen grotendeels bä nvloeden (zoals culturele waarden) scherp in de gaten dienen te worden gehouden. In veel gevallen betekent dit dat er nadrukkelijk aandacht moet zijn voor de vraag naar het *waarom:* waarom zijn er bepaalde regels in de offline wereld en waarom zouden deze regels in de online wereld gehandhaafd moeten blijven? Beleidsmakers moeten minder proberen de offline regels en belangen te transponeren naar de online wereld en meer oog hebben voor de eigenheid van de vraagstukken die in de online wereld spelen.

9.4.2 Overheidsregulering – marktregulering

We hebben hiervoor al aangegeven dat het reguleringsscenario van het primaat aan de markt in alle onderzochte landen plaats maakt voor een scenario waarin ook de overheid een duidelijke rol en functie heeft. In dit scenario van co-regulering trekken de overheid en de markt samen op bij het ontwikkelen van het beleid. Zoals hiervoor aangegeven stelden we overigens ook vast dat met de term co-regulering in de verschillende landen wel eens iets anders kan worden bedoeld.

Alhoewel als algemene beleidslijn het uitgangspunt van co-regulering wordt gepropageerd, blijkt bij een analyse van de specifieke onderwerpen en van de standpunten van de individuele landen, dat er ook belangrijke verschillen in de visie op regulering zijn te ontdekken. Bekeken vanuit de positie van de individuele landen, stellen we vast dat er landen zijn die op de lijn tussen overheidsregulering en marktregulering dichter bij het uitgangspunt van overheidsregulering zitten (Frankrijk), terwijl andere het primaat veel meer bij marktregulering leggen (Duitsland, VK en VS). Daarbij geldt tevens dat de voorkeur voor overheidsregulering dan wel marktregulering in belangrijke mate wordt bepaald door het specifieke onderwerp. De studie laat zien dat er een aantal onderwerpen is waarvan kan worden gesteld dat men

in de onderzochte landen in algemene zin meent dat een bepaalde mate van overheidsinterventie duidelijk gewenst is: consumentenbescherming, privacy en cybercriminaliteit. De belangen die hierbij een rol spelen zijn: rechtszekerheid, waarborgen van fundamentele rechten en plichten in de rechtsstaat en de nationale concurrentiepositie.

Bij de keuze voor een bepaalde mate van overheidsinterventie (bijvoorbeeld het stellen van bepaalde randvoorwaarden) ligt de vraag voor of men opteert voor een systeem van vrijwillig naleven van de gestelde regels of voor een systeem van verplichte naleving. In de onderzochte landen zijn verschillen waar te nemen in de mate waarin het naleven van bijvoorbeeld een certificeringsstelsel op vrijwillige basis kan (VK) dan wel verplicht wordt gesteld (Frankrijk). De ervaringen in het Verenigd Koninkrijk hierbij laten zien dat overheidsbeleid dat werkt met een systeem van vrijwillige medewerking door de private sector zeker effectief kan zijn: bedrijven en organisaties lijken zich aan dit beleid te willen conformeren omdat dit een concurrentievoordeel kan bieden. Gegeven juist dit aspect van concurrentievoordeel in combinatie met de mondiale markt van het Internet, kan een internationaal beleid dat uitgaat van vrijwillige medewerking voor bepaalde vraagstukken voordelen opleveren.

Het bovenstaande betekent voor het thema rechtsmacht en internationalisering dat de kans op succes van internationale harmonisatie mede afhangt van een duidelijk idee over de onderwerpen en gebieden waarover op supra-nationaal niveau overeenstemming bestaat. Daartoe is het van belang dat duidelijkheid bestaat over het gewenste niveau van aanpak (overheidsinterventie, co-regulering, pure zelfregulering), waarbij er oog is voor de diverse belangen en tradities die ten grondslag liggen aan de visie van de individuele nationale autoriteiten op het gewenste niveau van aanpak.

In het licht van het thema rechtsmacht en internationalisering wordt in de onderzochte landen niet gesignaleerd dat er mogelijk een negatief effect kan uitgaan van een al te ver doorgevoerd beleid inzake marktregulering. Volledige regulering door de markt zou immers het gevaar in zich kunnen hebben dat (onbedoeld) handelsbarrières worden opgeroepen. Te denken valt bijvoorbeeld aan een situatie waarin in de diverse landen verschillende voorwaarden voor het voeren van een keurmerk voor veilige elektronische handel worden gesteld. In het ene land kan daarmee aan bedrijven een hoger niveau van consumentenbescherming worden opgelegd dan in het andere land, hetgeen handelsbelemmerend zou kunnen werken.

9.4.3 Adagia – flexibiliteit

Daarmee komen we op het volgende onderscheid. Uit zowel de analyse van de diverse beleidsdocumenten in de onderzochte landen als de internationale workshop komt naar voren dat de overheid zich beter zou kunnen concentreren op het vinden van een op maat gesneden oplossing voor elk specifiek reguleringsvraagstuk in plaats van te proberen algemene richtlijnen en uitgangspunten voor het brede ICT-rechtsgebied te formuleren. Een kapstokbenadering in de zin van het hanteren van uniforme uitgangspunten bij het denken over regulering (zoals een algehele voorkeur voor zelfregulering en het adagium ‘online = offline’) doet onrecht aan de specifieke problematiek van de onderhavige materie.

Dit betekent niet dat in algemene termen geen voorkeur voor bepaalde uitgangspunten kan worden uitgesproken. Ter verduidelijking van het nationale overheidsstandpunt bij de internationale agendering van de problemen kan het zeker van waarde zijn bepaalde algemene standpunten (zoals co-regulering) te formuleren die de nationale belangen en tradities (qua cultuur en wetgeving) weerspiegelen, omdat men dan in internationale overleggen weet waar men aan toe is. De diversiteit aan problemen en nationale standpunten bij een internationale aanpak van de problemen

vraagt daarbij echter om een uiterst open houding die veeleer rekening houdt met mogelijke andere benaderingen en uitgangspunten dan vast blijft houden aan eigen uitgangspunten.

9.4.4 Antwoorden – sturen

Bij de vraag naar het waarom, kan ook worden gewezen op het conceptuele onderscheid tussen enerzijds regulering waarmee ten behoeve van bijvoorbeeld de rechtszekerheid wordt gepoogd een antwoord te geven op praktische vragen (bijvoorbeeld: "kan een elektronische handtekening worden ingezet voor het verrichten van rechtshandelingen?") en anderzijds regulering die beoogt gedrag te bë nvloeden (bijvoorbeeld: "gebruik geen encryptie die de opsporing belemmert"). Bij antwoordvraagstukken maakt het de rechtssubjecten in principe minder uit hoe de keuze uitvalt, als er maar een keuze gemaakt wordt; bij sturingsvraagstukken hebben de rechtssubjecten een duidelijke voorkeur voor een bepaalde richting. De overheid moet zich dus afvragen *waarom* het wenselijk is op een bepaalde manier in het maatschappelijk verkeer in te grijpen.

Voor het thema internationalisering en rechtsmacht betekent dit, dat overheden zich bewust moeten zijn van de mate waarin beoogde regulering antwoordt en de mate waarin beoogde regulering stuurt. Primair antwoordende regulering is op korte termijn gewenst om rechtszekerheid te garanderen; meer sturende regulering is pas gewenst als voldoende is uitgekristalliseerd welk doel wordt beoogd en wat daartoe het meest geëigende middel is.

Alhoewel in veel gevallen geen scherpe scheiding is aan te brengen tussen antwoordende en sturende regulering (zo zullen regels inzake de aansprakelijkheid van Internet-aanbieders deels antwoordend, deels sturend kunnen zijn), is het wenselijk dat de wetgever bij een eventueel regulerend optreden in ieder geval stil staat bij de vraag op welke kant van het spectrum antwoorden–sturen de nadruk van dit optreden ligt. Dit helpt hem bij het inschatten van de nalevingskans, de handhavingsmogelijkheden en dus de effectiviteit van de wetgeving.

9.4.5 Van bovenaf – van onderop

Sommige onderwerpen, zoals aansprakelijkheid voor Internet-aanbieders en elektronische handtekeningen, zijn als zodanig een nationaal vraagstuk dat in eerste instantie nationaal kan worden aangepakt. Vanwege de internationaliseringsdimensie is dat niet voldoende: de nationale aanpakken moeten ook internationaal op elkaar aansluiten. Dit wordt in internationale gremia gefaciliteerd. Aldus bestaat er een wisselwerking tussen de nationale en de internationale beleidsvorming, die parallel plaatsvinden. De wisselwerking vindt echter niet altijd optimaal plaats, zoals bij elektronische handtekeningen waarneembaar is: sommige nationale overheden (zoals Duitsland) hebben hier eerst een nationale oplossing gekozen die zij vervolgens internationaal als model hebben gepresenteerd, terwijl in internationale gremia (zoals de UNCITRAL) de gekozen oplossing een andere richting uitging. De benadering van onderaf had in dit geval dus te weinig oog voor de dimensie van internationalisering. De beleidsvorming zou in dergelijke gevallen aan slagkracht winnen als in een vroegtijdig stadium de benaderingen van onderop en van bovenaf meer op elkaar worden afgestemd.

Andere onderwerpen lenen zich echter per definitie voor een internationale aanpak, zoals het vraagstuk van toepasselijk recht bij online overeenkomsten en grensoverschrijdende satelliettaps. Bij deze onderwerpen vindt de beleidsvorming dan ook van bovenaf plaats, vanuit internationale organisaties. Opvallend is dat dit ertoe kan leiden dat nationale overheden hun inbreng in deze gremia niet expliciteren en

niet in hun beleidsdocumenten weergeven (zoals expliciete stellingnames over de Haagse Conferentie of het ontwerp-verdrag *Crime in Cyberspace*), waardoor de gedachtevorming en publieke discussie zich op nationaal niveau hier minder ontwikkelen dan bij de onderwerpen die een primair nationale component kennen. Dit kan uiteindelijk ook zijn weerslag hebben op de kwaliteit van de beleidsvorming op internationaal niveau. Ook hier zou dus een grotere wisselwerking tussen benaderingen van bovenaf en van onderop wenselijk kunnen zijn.

Het bovenstaande betekent dat het antwoord op de vraag welke onderwerpen in een vroeg stadium op de internationale agenda verschijnen te maken heeft met het (inter)nationaal handelingsvermogen. In de gevallen dat individuele landen de mogelijkheid hebben een probleem vooralsnog nationaal aan te pakken, zal de discussie op een internationaal niveau niet snel tot ontwikkeling komen. Dit houdt het gevaar in zich dat te snel een bepaald nationaal beleid wordt uitgezet. Een adequate aanpak van het thema internationalisering en rechtsmacht vraagt om een veel meer aandacht voor de internationale dimensie van alle problemen en een goede wisselwerking tussen de beleidsvorming op nationaal en die op internationaal niveau.

9.5 Verscheidenheid in eenheid

Welke algemene conclusies kunnen nu worden getrokken uit de veelheid aan specifieke conclusies? Wat betekent een en ander voor het centrale thema van deze studie 'rechtsmacht en internationalisering' en de nationale en internationale agendering van dit thema?

We menen te kunnen constateren dat er behoefte is aan een uniforme aanpak van de diverse problemen, maar dat daarbij vooral ook oog moet zijn voor de eigen dynamiek van de diverse onderwerpen, de diversiteit aan relevante belangen en de variëteit aan culturele en wetgevingstradities van de verschillende landen. Kortom: verscheidenheid in eenheid.

Dit betekent dat op diverse onderwerpen een internationale overeenstemming problematisch kan worden. Een creatieve aanpak in dit verband kan dan betekenen dat men allereerst op zoek gaat naar gebieden waarop relatief eenvoudig overeenstemming kan worden bereikt. Wanneer hierbij op hoofdlijnen over de principes overeenstemming is bereikt, kan vervolgens een onderwerp waarbij de standpunten meer divergeren ter hand worden genomen. Aldus kan het brede veld van ICT-recht in het licht van internationalisering en rechtsmacht stapsgewijs worden aangepakt.

Van groot belang daarbij is dat de diverse onderwerpen ook daadwerkelijk vanuit het *internationale* perspectief worden benaderd. Uit het onderzoek blijkt dat de gedachtevorming over ICT-recht nog steeds in belangrijke mate vanuit nationaal perspectief plaatsvindt, omdat men de zaken eerst nationaal op een rijtje wil zetten en vervolgens pas toe is aan internationale afstemming. In het licht van het "opgroeien" van ICT-recht is dat niet verwonderlijk, maar het is onwenselijk om nog langer het internationale perspectief buiten het blikveld te houden. De vraagstukken van internationalisering en rechtsmacht zijn dermate inherent aan beleidsvorming op ICT-rechtsgebied, dat het nationale en het internationale perspectief niet zonder elkaar kunnen.

Wij menen dat het hoog tijd is voor de volgende stap bij het reguleren van de elektronische snelweg. Vijf jaar geleden was het beleid geconcentreerd op de aanpak van nationale problemen. Nu deze aanpak goed op weg is, wordt het tijd voor de volgende stap: de internationale dimensie van de problemen. Alhoewel de diverse

overheden momenteel wel roepen dat er tot een internationale afstemming van het beleid dient te worden gekomen, blijkt uit deze studie dat in concreto nog weinig van de grond komt en dat wordt opgemerkt dat de problemen allereerst op nationaal niveau moeten uitkristalliseren. De onderwerpen die momenteel op de agenda van de diverse internationale gremia staan, betreffen veelal niet de meest fundamentele problemen inzake internationalisering en rechtsmacht, en voorzover ze wel op de agenda komen (zoals internationaal privaatrecht) blijkt overeenstemming nog ver te zoeken. Veel activiteiten binnen internationale organisaties hebben dan ook vooral beleidsvoornemens en globale principes opgeleverd, maar nog weinig concrete resultaten. Kortom, op nationaal en op internationaal niveau vindt vooralsnog te weinig effectieve gedachtevorming plaats over het beleid op het thema internationalisering en rechtsmacht.

De Nederlandse overheid zou daarom internationaal moeten aandringen op structurele aandacht voor het perspectief van internationalisering en rechtsmacht in alle fora waar onderwerpen op ICT-rechtsgebied worden besproken. Ook zou de Nederlandse overheid zich sterk moeten maken om de beleidsvorming in de vele verschillende internationale instanties en fora beter op elkaar af te laten stemmen. Voor de helderheid van de discussie en de beleidsvorming kan het daarbij zinvol zijn uitgangspunten te formuleren die de Nederlandse standpuntbepaling op deze onderwerpen ondersteunen. Deze uitgangspunten kunnen internationaal een aanknopingspunt vormen voor het vaststellen welke belangen internationaal breed worden gedeeld; vandaaruit kan dan worden bepaald welke onderwerpen op internationaal niveau met een redelijke kans van slagen geregeld kunnen worden. Voorlopig moet daarbij vooral de aandacht worden gericht op "antwoordvraagstukken" en minder op "sturingsvraagstukken".

Uitgangspunten voor standpuntbepaling en beleidsvorming rond vraagstukken van internationalisering en rechtsmacht mogen echter nooit meer zijn dan startpunten voor discussie. Voor alles moeten overheden in de internationale discussies, meer nog dan bij traditionele rechtsonderwerpen, een flexibele en vooral open houding hanteren die oog heeft voor alle nuances van het onderwerp en de variëteiten van de nationale standpunten die eigen zijn aan de problematiek van internationaliseringvraagstukken rond ICT-recht.

De slotconclusie luidt dat overheden de internationale dimensie nadrukkelijker moeten betrekken bij de nationale en de internationale beleidsvorming op ICT-rechtsgebied. Het ICT-recht is inmiddels te groot geworden voor de kinderschoenen van algemene uitgangspunten en nationale interim-oplossingen. Een volwassen ICT-recht vraagt om structurele inbedding van het perspectief van internationalisering en rechtsmacht.

Summary

The information society is essentially an international society. This challenges the law, which is still to a large extent nationally-based. How can and should governments regulate information and communications technologies (ICT) and the Internet, given the fundamental influence of internationalisation? This research presents the points of view on this of the governments of France, Germany, the United Kingdom, and the United States, focusing on a number of general themes and specific issues in private and criminal law. The research was commissioned by the Dutch Ministry of Justice to support their memorandum *Internationalisation and the law in the information society* of May 2000. It took place from January through April 2000 by analysing the states' major ICT policy papers and laws and by an international workshop held in Amsterdam[246].

General themes

Unlike the Dutch government, which published an overall analysis of ICT law in 1998 (*Legislation for the electronic highways*), few comprehensive legal policy documents avail in the countries researched; only France has taken a similar effort with its *Policy Paper On The Adaptation Of The Legal Framework To The Information Society* of October 1999, which is to lead to a draft law in 2000.

Nevertheless, the general treatment of ICT law in view of internationalisation in France, Germany, the UK, and the US is roughly the same. This holds, for instance, for the first general theme researched, the principle that "what holds offline, should also hold online". This is the basic starting point of Dutch policy. It is also explicitly mentioned in the policy of the UK, whereas it can be derived implicitly from the policy documents and laws of France and Germany. However, in recent times, the adage has been put under pressure, because legislative initiatives on several specific issues show that it is not always followed. Increasingly, certain interests – such as consumer protection, legal certainty, stimulating electronic commerce – call for specific rules for the online world that differ from those in the offline world. This tendency is also mirrored at the international level, e.g., in the European Union.

It is true that the adage "what holds offline, should also hold online" was a useful concept in the "early days" of ICT law (in the mid 1990s), when it had to be made clear that the Internet was not a legal vacuum. Now, however, it appears rather a romantic, outdated concept. The complexity of the matter proves that the problems in the online world differ from those in the offline world. Therefore, it is unwise to take as a starting point the concrete rules of the offline world when thinking about regulating the online world. Rather, the levels of protection should be the same in both worlds (as US policy documents mention). Governments should pay more attention to the interests and goals underlying the rules of the offline and online worlds. The question is *why* we have certain rules in the offline world, and *why* such rules should be maintained online. Rather than rely on transposing traditional rules or

[246] A report in English of the workshop is presented in Appendix IV.

principles, governments had better forget the adage and be simply creative in finding solutions to the specific problems of the online world. One must also bear in mind the possibility that the adage "what holds offline, should also hold online" may be turned into its reverse: "what holds online, should also hold offline". Thus, the legislative must view the relationship between offline rules and online rules as an interactive one.

The second general theme of this research is self-regulation. The Dutch government has appeared a fervent adherent of self-regulation mechanisms in solving legal uncertainty about the consequences of cross-border electronic communications. In choosing self-regulation, the government hopes to create sufficient flexibility in a time of technological and societal turbulence. Also, self-regulation is, in principle, not bound by borders. Nevertheless, government regulation is still the starting point if fundamental values of the rule of law are at stake – the Dutch government here refers to the classic fundamental civil rights, to preventing and investigating breaches of the rule of law and of state security, as well as to consumer protection, privacy, and the issue of applicable law.

The research shows that self-regulation is likewise a central theme in the various policy documents of the countries as well as of international organisations. Also, more or less the same issues are mentioned when it comes to a preference for government intervention (in particular, fundamental rights and values, consumer protection, law and order, state security).

Despite the broad support for self-regulation, there is a remarkable tendency in all countries. Whereas the governments used to take the point of view that government intervention was, in principle, undesirable and that the market should lead, there is increasing awareness that governments cannot restrict themselves to solely stimulate; shaping e-commerce policy and Internet policy is a task for government and market together. 'Co-regulation' is a term that appears prominently in many recent policy documents. Even in the US, the general opinion seems to tend to a view that the government should play a more guiding role than it used to do in shaping the policy. One must bear in mind, however, that the term 'co-regulation' is not interpreted the same way in the various countries. The interpretation depends to a large extent on legislative and cultural traditions. When governments talk about co-regulation, they are therefore prone to talk about different things.

In thinking about the necessity of government intervention, it may be useful to distinguish between regulation that aims at answering practical questions ("Can I use a digital signature to make a transaction?") and regulation that aims at influencing behaviour ("Don't use encryption that hampers law enforcement!"). The first kind of regulation is generally called for and welcomed by the market, whereas the second kind is generally not favoured.

When deciding both what rules should apply in the online world and what level of regulation can best shape these rules, the enforcement of the resulting regulation is of crucial importance. Especially in an international context, enforcement of regulation is a problematic issue. This, then, is a third general theme that pervades ICT law.

In the policy documents, the question of how to safeguard enforcement is less prominent than the first two general themes. Although governments have put considerable thought to the necessity and options of ensuring enforcement of ICT law in the international context, so far, they have not put forward ideas about an integral approach to enforcement. They simply look for the best approach in each given case, which is in line with the Dutch pragmatic approach in this matter. It is also remarkable that there are few concrete ideas about how to address at an international level those issues generally considered to be potentially difficult to enforce in an international context, such as tax law, privacy, and cryptography.

In those areas where the interests to be protected are broadly shared internationally, there will be the best likelihood of an international approach. It is wise to start with small domains on which there is more agreement, e.g., in combating child pornography, for which an international network of hotlines is already at work. Constructions of national contact points are the most promising in the short term to address enforcement internationally. In private-law matters, one can think of an international network of ombudspersons or Chambers of Commerce to play a central part in international alternative dispute resolution. In criminal law, for the time being, states concentrate on an international network of national contact points available 24 hours a day and seven days a week to directly deal with and co-ordinate requests for mutual criminal assistance. This network can give an impetus to further-reaching forms of cross-border co-operation.

Specific issues

Besides these general themes, we researched four specific issues, two in criminal law and two in private law.

The first issue in criminal law is double criminality, which is usually required for mutual assistance in criminal matters. In the memorandum *Legislation for the electronic highways*, the Dutch government suggested that this requirement could perhaps be dropped under certain conditions in cases where a state requests another state to provide information in order to be able to follow a digital trace.

There is no indication that other countries think about abandoning the requirement of double criminality. It is true that within the Council of Europe, it is discussed, but overall their draft *Convention on Cyber-Crime* (usually referred to as *Crime in Cyberspace*) does not initiate discarding double criminality. Although the text seems to suggest that the requirement must not or need not be absolute, there is no consensus on this among the participating states. Moreover, the abandonment of double criminality as discussed is restricted to *preserving* data in another country; it does not stretch to *providing* those data, and so, the requirement will at all counts continue effectively to exist.

Likewise, the discussion at the international workshop did not support relinquishing the requirement of double criminality. The foreign experts appeared surprised rather than stimulated to think about the idea. Double criminality seemed to them to be so fundamental, that there is or should be in fact no possibility to undermine it in any way.

Given the fact that abandoning double criminality in any way is not favoured internationally, and because of the fact that in most cases it is hardly realistic to harmonise material criminal laws, the international fight against ICT crime will have to resort to co-operation between enforcement authorities.

The Dutch government's view on this second issue, co-operation between enforcement authorities, is that there must be rules that ensure effective co-operation, especially to regulate investigation powers aimed at foreign Internet providers and to ensure the co-operation of other states to facilitate investigation. In particular, the government stated in its 1998 memorandum that the draft treaty *Crime in Cyberspace* should enable judicial authorities to directly address foreign network providers, without prior mediation of investigation authorities in the country of the network provider. Court supervision could take place afterwards.

The necessity of closer co-operation between enforcement authorities is recognised in the other countries. Governments acknowledge that to achieve this, traditional mutual assistance will have to be adapted drastically. They see this primarily as a problem for which solutions have to be found at an international level. Therefore,

this issue is discussed mainly in international platforms; on the national level, no conclusive steps are taken before the results of the international discussions become clear.

At a national level, states restrict themselves to short-term measures, like establishing continuously accessible contact points, and to other means available within the present legal framework. The Dutch desire to make it easier to gain access to foreign data seems to be in line with the thinking in other countries, but foreign governments have not yet published positions about the specific desire to get data directly from foreign Internet providers.

Moreover, the draft convention *Crime in Cyberspace* of the Council of Europe does not contain a proposal to this effect. It does propose a new investigation power: a preservation order to telecoms or Internet providers that can be easily given and that safeguards the availability of the data pending the exercise of other investigation powers, such as a search and 'seizure' of data. However, for preserving data stored in another state, authorities will still have to make a traditional request for criminal assistance – a request addressed to foreign providers directly was turned down in the draft convention.

The first specific issue in private law we researched is the topic of applicable law in international online contracts. The Dutch government attaches great value to clarifying the rules of private international law on which law applies. The Dutch government favours establishing a broadly formulated framework of private international law rules that apply to online contracts within the framework of the Hague Conference on private international law.

For the time being, this view does not seem to be shared in the countries we researched. In the US, the issue does not seem to play a part in policy-making at the federal level (bearing in mind that in the US, the issue of applicable law to online contracts can be addressed at the state level). For Germany and the UK, we did not find government positions on this, whereas France has formulated a different position. The European countries seem to want to tie in with the existing rules of the (European) Rome Convention. The Netherlands, then, is leaning more towards a global solution than the other countries. One should note, however, that this approach does not seem to work out particularly smoothly. At a meeting in Ottawa in February 2000, it appeared scarcely realistic to agree upon the draft for adapting the Hague Conference.

The second issue in private law is civil liability of Internet providers. In Dutch law, tort is sufficiently technology-independent for the government to be able to leave it to the courts to develop this issue. Still, the government supports the European Commission in trying to establish common principles at an international level in order to create a level playing field. However, the Dutch government does not agree with all proposals on provider liability in the draft E-Commerce Directive. In particular, the Minister of Justice questions the clarity of the distinction between the various categories of service providers (access, caching, and hosting providers). Moreover, he doubts the prudence of excluding beforehand access providers from liability regardless of whether they had knowledge of illegal content.

An analysis of the civil-liability position of Internet providers in the other countries shows that the material criteria used are similar, for instance, involvement with the content, knowledge, and due care. Providers that are involved with the content are fully liable, while those that are not are only liable if they do not conform with duties of care. In some countries, the latter category further distinguishes between access providers and hosting providers. Generally, (non-content) providers are only liable for illegal content of which they have knowledge, with two exceptions. In Sweden, providers have a pro-active duty to check material; since they can comply with this requirement by establishing a hotline, there is no obligation of result but only

one of effort. A second exception is the categorical exclusion, regardless of knowledge, of access providers in the German and EU regulations. Finally, a duty of care for service providers encountered everywhere is to remove or block access to illegal content as soon as the provider gains knowledge of it, at least as far as he is reasonably able to.

It is generally recognised that Internet service providers have a special role and responsibility to identify content providers. This may also stretch to preparatory measures like preserving data and verifying the identity of new subscribers. However, most governments are still struggling to find a balance between this requirement and the resulting infringement of privacy regulations.

There is sufficient space for regulating provider liability within each national state. However, to prevent major differences between the national regulations (which could impede international e-commerce), international harmonisation is called for, hence the regulation in the European E-Commerce Directive.

As to the international problems of illegal content – addressing content that is illegal in a country but that is hosted abroad – the general position of governments is one of reserve. States do not view provider liability a good way to address this (it is interesting to note that Australia and Singapore are exceptions to this, with regulations that put obligations on national providers with respect to content hosted abroad). For the time being, states take recourse to stimulating international co-operation between private-sector hotlines.

Conclusions

The findings of the research suggest that several distinctions and trade-offs are relevant to creating ICT-law policies.

- **Offline online**: the adage "what holds offline, should also hold online", a useful concept in the early days of ICT law, appears not to be generally applicable anymore. It is still relevant in relation to the interests and the level of protection that underlie the rule systems of the offline and online worlds, but rather than focusing on transposing the offline rule system to the online world, governments should focus on the specificity of the problems in the online world.
- **Government regulation self-regulation**: the general preference for self-regulation that until recently pervaded thinking about ICT law is generally giving way to a preference for co-regulation, since governments have come to the conclusion that safeguarding crucial interests and legal certainty calls for a more prominent role of governments. This new balance between government and market regulation is termed co-regulation everywhere, but the specific interpretation of this term varies per country. Some countries put more stress on the government side, and others on the market side, largely because of their cultural and legislative traditions. This influences, among others, the choice of a voluntary or an obligatory enforcement mechanism. From an international perspective, it is important to be aware of the variation in the views on co-regulation and in the underlying national values.
- **Overall principles specific solutions**: governments had better concentrate on finding a tailor-made solution to each specific issue requiring regulation rather than try to define general guidelines and principles for the broad field of ICT law. General principles (such as an overall preference for self-regulation and "offline = online") do injustice to the specific problems of all the various issues. In order to make clear the government position in international platforms, it may be useful to define certain general positions that mirror national interests and traditions, but this holds the risk that national governments sticking to their general position as

outlined hamper the search for a creative solution. It is more important in international platforms for governments to have an open attitude that takes into account other valid approaches and principles.

- **Answering steering:** conceptually, one can distinguish between regulations that primarily try to answer practical questions in order to create legal certainty (e.g., "can I use a digital signature to sign a contract?") and regulations that aim at influencing behaviour (e.g., "do not use encryption that hampers investigation"). With 'answering issues', the addressees, in principle, care less about the particular outcome as long as a choice is made by the government, whereas with 'steering issues', addressees have a clear preference for a particular outcome. It is true that regulation is never completely answering or completely steering, but in most cases, there is an emphasis on one side or the other. This affects the likelihood of compliance, the enforcement options, and therefore the effectiveness of the regulation. In the short term, primarily answering regulations are called for in order to establish legal certainty, whereas more steering regulations should only be undertaken once it has become sufficiently clear what 'steering goals' are envisioned and what are the best means to achieve those goals.
- **Top-down bottom-up**: certain topics, such as Internet-provider liability and electronic signatures, are essentially national issues that can be addressed at a national level; given the fact of internationalisation, however, these national regulations must be tuned to one another, which is done at an international level. The resulting interaction between national and international actions is not always optimal, because states sometimes at an early stage create national legislation that significantly diverges from solutions proposed internationally.
  Other topics call for an international approach by definition, such as applicable law in online contracts and cross-border satellite eavesdropping. In these areas, policies are made nearly only at the international level, which holds the risk that national governments do not publish their opinions and do not trigger a national debate on these topics. This can also hamper the interaction between national and international policy-making. Both the primarily bottom-up issues and the primarily top-down issues, then, call upon governments to be more aware of the international dimension of the policies under discussion, and to optimise the interaction between national and international policy-making.

What conclusions can be drawn from this analysis? We discern a desire for a uniform approach of the various problems, but at the same time a need to be aware of the specific dynamics of each issue, the range of interests involved, and the variety of cultural and legislative national traditions. In short, there must be variety in unity.

This means that in various areas, international agreement can be problematic. The creative approach that is needed implies in the first place a search for areas where the interests are mutual and where it is relatively easy to reach agreement. Once governments agree upon the major points in this area, topics could be addressed where the positions diverge more. The broad field of ICT law must thus be addressed slowly, step by step.

It is of primary importance that each issue is indeed addressed from an international perspective. Our research indicates that the thinking about ICT law is still taking place to a large extent from a national perspective. This is not surprising in the light of the 'growing-up' of ICT law, but it is undesirable to keep the international perspective out of sight any longer. Questions of internationalisation and jurisdiction are so intrinsic to policy-making in the area of ICT law, that the national and international perspectives cannot do without each other.

We think the time has come to make the next step in regulating the electronic highway. Five years ago, policy concentrated on addressing national problems. Now

that this approach is well on its way, it is time for the next step: including the international dimension of the problems. Although governments currently proclaim that international policy fine-tuning is needed, our analysis shows that in reality, few things come off the ground, and that it is often noted that problems should first take shape at a national level. There are many initiatives by international organisations, but these have yielded few concrete results so far. In short, both at the national and at the international level, there is little effective progress in policy-making from the perspective of internationalisation and jurisdiction.

The Dutch government should therefore urge the international community to structurally pay attention to the perspective of internationalisation and jurisdiction in all the platforms that discuss ICT-law issues. Also, the Dutch government should make a case for better tuning of the policy-making in all the various international institutions and platforms. In order to facilitate the international discussions in which it takes part, the Dutch government's formulation of rules of thumb that support the Dutch positioning may be useful, but these can be no more than starting points for discussion. First and foremost, and even more so than with traditional law topics, the government should have a flexible and particularly open attitude that discerns and pays attention to all the nuances of the issue at stake and the variety of national positions that are intrinsic to the internationalisation problems related to ICT law.

The final conclusion is that governments should incorporate the international dimension more emphatically in the national and international policy-making in the field of ICT law. ICT law has by now outgrown the infancy stage of general starting points and national interim solutions. A grown-up ICT law calls for structurally incorporating the perspective of internationalisation and jurisdiction.

Literatuur

Asscher 2000
Lodewijk Asscher, 'Naar een eEurope van de burgers!', *Nederlands Juristenblad* 2000, p. 762-763.

Battle 1998
John Battle, *HMG Strategy For the Internet*, 18 maart 1998, WWW <http://www.dti.gov.uk/Minspeech/btlspch3.htm>.

Bertelsmann 1999
Bertelsmann Foundation, *Self-regulation of Internet Content*, Gütersloh 1999, verkrijgbaar op WWW <http://www.bertelsmann-stiftung.de/internetcontent/english/content/c3200.htm>.

Blair 1998
Tony Blair, *Our Information Age, The Government s Vision*, mei 1998, WWW <http://www.number-10.gov.uk/textsite/info/releases/publications/infoagefeat.html>.

BMBF 1999
Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, *Multimedia möglich machen. Deutschlands Weg in die Wissensgesellschaft*, februari 1999, WWW <http://www.iid.de/mmm_bmbf/mm_p4.htm>.

BMWi 1996
Bundesministerium für Wirtschaft, *Info 2000: Deutschland s Weg in die Informationsgesellschaft*, februari 1996, WWW < http://www.bmwi-info2000.de/archive/berichte/info2000/index.html>

BMWi 1999
Bundesministerium für Wirtschaft und Technologie, *Evaluierungsbericht des IuKDG*, 16 juni 1999, WWW <http://www.iid.de/iukdg/pm160699.html>.

Den Boer 1999
M.G.W. den Boer, 'Internationale politiesamenwerking', in: C.J.C.F. Fijnaut, E.R. Muller & U. Rosenthal (red.), *Politie. Studies over haar werking en organisatie*, Alphen a/d Rijn: Samsom 1999.

Bundesregierung 1999
Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts Aktionsprogramm der Bundesregierung, 1999, <http://www.iid.de/aktionen/aktionsprogramm/deckblatt.html>.

Cabinet Office 1999
Cabinet Office, *E-commerce@its.best.uk*, september 1999, WWW <http://www.cabinet-office.gov.uk/innovation/1999/ecommerce/index.htm>.

CISI 1999
Comité Interministériel pour la Société de l'Information, *Mise en oeuvre du Programme d action gouvernemental pour la société de l information Etat d avancement après un an (janvier 1998 janvier 1999)*, 19 januari 1999, WWW <http://www.internet.gouv.fr/francais/textesref/cisi190199/sommaire.htm>.

Clarke 1999
C. Clarke, *Speech to the International Hi-Tech Crime and Forensic Conference*, 4 oktober 1999, WWW <http://www.infowar.com/law/99/law_100799d_j.shtml>.

Clinton 1997
William J. Clinton, *Presidential Directive*, 1 juli 1997, WWW <http://www.whitehouse.gov/WH/New/Commerce/directive.html>.

Conseil d'Etat 1998
Conseil d'Etat , *Internet et les résaux numériques*, 2 juli 1998, WWW <http://www.internet.gouv.fr/francais/textesref/rapce98/synthese.htm>.

Council of Europe 1995
Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology, 11 september 1995, WWW <http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html>.

Council of Europe 2000
Council of Europe, *Crime in Cyberspace. First Draft of International Convention Released for Public Discussion*, 27 april 2000, WWW <http://conventions.coe.int/treaty/en/projets/cybercrime.htm>.

Department of Commerce 1997
Department of Commerce, *Privacy and Selfregulation in the Information Age*, juni 1997, WWW <http://www.ntia.doc.gov/reports/privacy/privacy_report.htm>.

Department of Commerce 1998
Department of Commerce, *The Emerging Digital Economy*, april 1998, WWW <http://www.ecommerce.gov/emerging.htm>.

Department of Justice 1999
Justice Department comments to the FTC on Consumer Protection in the Global Marketplace, 29 maart 1999, WWW <http://www.usdoj.gov/criminal/cybercrime/ftcconsu.htm>.

DPWP 1999
Data Protection Working Party, *Recommendation on the Respect of Privacy in the context of Interception of Telecommunications*, 3 mei 1999, WWW <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp18en.htm>.

Drion 1999
C. Drion, 'Internationale ontwikkelingen in materieel recht met betrekking tot e-commerce, over botsende rechtsstelsels en het "compartimenteringsbeginsel" en

enkele specifieke vragen van internationaal privaatrecht', in: *Meester over 2000, Meester over IT* (Jonge Balie Congres 1999), Den Haag: Sdu 1999, p. 67-85.

Enquete-Kommission 1998
Schlußbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft Deutschlands Weg in die Informationsgesellschaft zum Thema Deutschlands Weg in die Informationsgesellschaft, 22 juni 1998, Druksache 13/11004.

Eijlander e.a. 1993
Ph. Eijlander, P.C. Gilhuis, J.A.F. Peters (red.), *Overheid en zelfregulering*, Zwolle 1993.

Van Esch 1999
R.E. van Esch, *Electronic Data Interchange (EDI) en het vermogensrecht*, diss. Nijmegen, Deventer: Tjeenk Willink 1999.

FCC 1997
Federal Communications Commission, *Digital Tornado: The Internet and Telecommunications Policy*, maart 1997, WWW
<http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf>.

G8 1999
Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, October 19-20, 1999, *Communiqué*, WWW
<http://www.library.utoronto.ca/g7/adhoc/crime99.htm>.

Den Haan 1998
Reinoud den Haan, *Internationale organisaties en de elektronische snelweg*, november 1998 (rapport voor Ministerie van Justitie, ongepubliceerd).

Van der Hof 1998
S. van der Hof, 'De Internetconsument en het internationaal privaatrecht, *Tijdschrift voor consumentenrecht*, december 1998, nr. 5, p. 415-21.

Van der Hof 2000
S. van der Hof, 'De Internationale on-line overeenkomst', in: *De e-Consument. Consumentenbescherming in de Nieuwe Economie* (preadvies NVvIR), Elsevier 2000.

Hogan 1999
S.B. Hogan, 'To Net or Not To Net: Singapore's Regulation of the Internet', *Federal Communications Law Journal* 1999, p. 429-447, WWW
<http://www.law.indiana.edu/fclj/pubs/v51/no2/v51no2.html>.

Holder 1999
Eric Holder, *International Conference Combating Pornography on the Internet . Remarks of U.S. Deputy Attorney General Eric Holder*, Vienna, 29 september 1999, WWW
<http://www.usdoj.gov/criminal/cybercrime/dagceos.html>.

House of Lords 1996
House of Lords, *Information Society: Agenda for Action in the UK*, 23 juli 1996, WWW
<http://www.parliament.the-stationery-office.co.uk/pa/ld199596/ldselect/inforsoc/inforsoc.htm>.

House of Commons 1999
House of Commons, *Tenth Report of the Select Committee on Trade and Industry*, augustus 1999, WWW <http://www.parliament.the-stationery-office.co.uk/pa/cm199899/cmselect/cmtrdind/648/64802.htm>.

Hugot 1999
Rapport numéro 154 de M. Jean-Paul HUGOT, fait au nom de la commission des Affaires culturelles, 22 december 1999, WWW <http://www.senat.fr/rap/l99-154/l99-154.html>.

ICANN 1999
ICANN, *Uniform Domain Name Dispute Resolution Policy*, 24 oktober 1999, WWW <http://www.icann.org/udrp/udrp-policy-24oct99.htm>.

ISI 1999
The Government s policy for the information age, WWW <http://www.isi.gov.uk/isi/infosoc/govpolicy.htm> (inzage 26 april 2000).

Jabbour 1999
V. Jabbour, 'Comment on the interception of communications in the UK Consultation Paper', *Computer Law & Security Report* 1999, p. 389-391.

Jansen & Janssen 1999
Buro Jansen & Janssen, *Luisterrijk. Een gids over afluisteren*, Amsterdam: Jansen & Janssen/ Papieren Tijger 1999.

Jospin 1997
Prime Minister, 'Preparing France's Entry into the Information Society', 25 augustus 1997, WWW <http://www.premier-ministre.gouv.fr/GB/INFO/HOURT.HTM>.

Jospin 1999a
Le Premier Ministre, *Société de l information: discours du Premier ministre à l Université d été de la communication*, Hourtin, 26 augustus 1999, WWW <http://www.internet.gouv.fr/francais/textesref/pagsi2/discourspm.htm>.

Jospin 1999b
Le Premier Ministre, *Allocution du Premier ministere lors de la réception concluant la conférence mondiale des régulateurs sur l internet*, Paris, 1 december 1999, WWW <http://www.premier-ministre.gouv.fr/PM/D011299.htm>.

Judicial Co-operation Unit 1999
Judicial Co-operation Unit, *Seeking Assistance in Criminal Matters from the United Kingdom. Guidelines for judicial and prosecuting authorities (Second Edition)*, oktober 1999, WWW <http://www.homeoffice.gov.uk/oicd/jcu/guidelns.htm>.

Koops 2000
B.J. Koops, *Crypto Law Survey*, versie 17.0, februari 2000, WWW <http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>.

KPMG & Denton Hall 1999
KPMG en Denton Hall, *Review of the Internet Watch Foundation. A report for the DTI and Home Office by KPMG and Denton Hall*, z.d., WWW <http://www.kpmgiwf.org/iwfrevu.pdf> (inzage 26 april 2000).

Linklaters & Alliance 1999
Linklaters & Alliance, *Telecommunications and electronic business: doing business in the electronic age. A legal overview*, Deventer: Kluwer 1999.

Lorentz 1998a
Ministère de l'Économie, des Finances en de l'Industrie, Francis Lorentz, *Commerce électronique. Une nouvelle donne pour les consommateurs, les entreprises, les citoyens et les pouvoirs publics*, 7 januari 1998, WWW <http://www.finances.gouv.fr/lorentz/rapports/index-d.htm>.

Lorentz 1998b
Ministère de l'Économie, des Finances en de l'Industrie, Francis Lorentz, *Rapport sur le commerce électronique Addendum*, 15 maart 1998, WWW <http://www.finances.gouv.fr/lorentz/rapports/forum.htm>.

Lorentz 1999
Ministère de l'Économie, des Finances en de l'Industrie, Francis Lorentz, *La nouvelle donne du commerce électronique. Réalisations 1998 et perspectives. Synthèse*, februari 1999, WWW <http://www.finances.gouv.fr/lorentz/travaux/synth_generale.html>.

Nota WES
TK 1997-1998, 25 880, nrs. 1-2 (*Wetgeving voor de elektronische snelweg*).

OECD 1997
OECD, *Recommendation of the Council concerning Guidelines for Cryptography Policy*, 17 maart 1997, WWW < http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm>.

OECD 1998a
OECD, Working Party on Information Security and Privacy, *Ministerial Declaration On the Protection Of Privacy On Global Networks*, DSTI/ICCP/REG(98)10/FINAL, 18 december 1998, WWW <http://appli1.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)10-final>.

OECD 1998b
OECD, *Ministerial Declaration On Consumer Protection in the Context Of Electronic Commerce*, DSTI/CP(98)12/FINAL, 18 december 1998, WWW <http://www.olis.oecd.org/olis/1998doc.nsf/LinkTo/DSTI-CP(98)12-FINAL>.

OECD 1998c
OECD Ministerial Conference Ottawa, *A Borderless World: Realising the Potential of Global Electronic Commerce*, 7-9 oktober 1998.

OECD 1998d
OECD Ministerial Conference Ottawa, *A global action plan for electronic commerce prepared by business with recommendations for Governments*, 7-9 oktober 1998.

OECD 1999
OECD Forum on Electronic Commerce, *Report on the Forum*, Parijs, 12-13 oktober 1999.

PAGSI 1998
Comité Interministériel pour la Société de l'Information, *Programme d action gouvernemental. Préparer l entrée de la France dans la société de l information*, 16 januari 1998, WWW <http://www.internet.gouv.fr/francais/textesref/pagsi.htm>.

Palme 1998
J. Palme, *Swedish Law on Responsibilities for Internet Information Providers*, bijgewerkt 3 juni 1998, WWW <http://www.dsv.su.se/~jpalme/society/swedish-bbs-act.html>.

Polak 1998
M.V. Polak, 'Internationaal privaatrecht: vangnet voor het Internet', *Nederlandse Juristen-Vereniging 1998-I*, Deventer: Tjeenk Willink 1998, p. 59-118.

President's Working Group 2000
President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet* , maart 2000, WWW <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>.

Prins & Gijrath 2000
J.E.J. Prins & S.J.H. Gijrath, *Privaatrechtelijke aspecten van elektronische handel*, Deventer: Tjeenk Willink 2000.

Prins & Van Kralingen 1997
J.E.J. Prins & R.W. van Kralingen, 'De invloed van informatie- en communicatietechnologie op het recht', in: *Volatilisering in de economie*, Den Haag: WRR 1997, p. 121-122.

Scott 1999
B. Scott, 'An Essential Guide to Internet Censorship in Australia', *World Internet Law Report* 1999/10, p. 16-21.

Sieber 1998
U. Sieber, *Legal aspects of computer-related crime in the Information Society comcrime study* , 1998, WWW <http://www2.echo.lu/legal/en/comcrime/sieber.html>.

STOA 1998
Steve Wright, Omega Foundation, *An appraisal of technologies for political control. Working document*, Luxembourg: European Parliament B STOA, 6 januari 1998, WWW <http://jya.com/stoa-atpc.htm>.

STOA 1999
Duncan Campbell, *Interception Capabilities 2000. Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programme office) on the development of surveillance technology and risk of abuse of economic information*, april 1999, WWW <http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm>.

Strauss Kahn e.a. 1999
Dominique Strauss Kahn et al., *Une société de l information pour tous. Document d orientation*, november 1999, WWW <http://www.internet.gouv.fr/francais/index.html> (Engels: *Policy Paper On The Adaptation Of The Legal Framework To The Information Society*, WWW <http://www.finances.gouv.fr/societe_information/anglais/sommaire_ang.htm>).

White House 1997
William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce*, 1 juli 1997, WWW <http://www.whitehouse.gov/WH/New/Commerce>.

White House 1998
The White House*, Memorandum for Heads of Executive Departments and Agencies*, 1 mei 1998, WWW <http://www.npr.gov/library/direct/memos/disputre.html>.

White House 1999
The White House, *Memorandum for the Heads of Executive Departments and Agencies. Facilitating the Growth of Electronic Commerce*, 29 november 1999, WWW <http://www.whitehouse.gov>.

White House 2000
The White House, *National Plan for Information Systems Protection*, 7 januari 2000, verkrijgbaar via WWW <http://www.epic.org/security/infowar/resources.html>.

Bijlage I – Overzicht van overheden over ICT-recht en –beleid

	Duitsland	**Frankrijk**	**VK**	**VS**
algemene visie	internationale aanpak, waarbij nationale aanpak als model kan (of moet) fungeren	internationale samenwerking, waarbij er ruimte is voor nationale pluriformiteit	internationale samenwerking is noodzakelijk	internationale aanpak, waarbij zelfregulering hoge prioriteit heeft
belangen	rechtszekerheid, publiek belang (o.a. consumentenbe-scherming, Jugendschutz)	marktwerking en stimulering van bedrijven, mensenrechten, consumenten-bescherming, culturele traditie	publiek belang, met name obsceniteit en marktwerking en stimulering van bedrijven	pluriformiteit van informatie, stimuleren marktwerking, consistent juridisch raamwerk, consumentenbesche rming, bescherming minderjarigen
doel en strategie	nationale wetgeving als model; Europa moet in internationale gremia meer sturen en beïnvloeden om invloed van Europa te vergroten; wereldtop 2002 (ITU) heel belangrijk, nauwe betrokkenheid bij agendavorming	actieve deelname in internationale fora om Franse belangen te waarborgen; Europa moet in internationale gremia integrale houding innemen en meer sturen en beïnvloeden; goed evenwicht vinden tussen communautaire harmonisatie en resterende nationale wetgeving	leidende rol in internationale fora; Europese Commissie moet actiever participeren in Global Business Dialogue om invloed van Europa en Europese bedrijven te vergroten	wegnemen van buitenlandse handelsbelermmerin gen; overtuigen van buitenland dat inzet op zelfreguleringsmecha nismen e-handel het best bevordert
e-handel	spitst zich vooral toe op belasting, consumenten-bescherming (transparantie is belangrijk) en privacy; op internationaal niveau moet één internationale instantie weblocatie-keurmerken afgeven volgens internationaal afgestemde criteria	er moet meer lijn komen in gefragmenteerde initiatieven in diverse internationale gremia; er moet één Europees raamwerk komen, met belangrijk basisprincipe consumentenbesche rming; bij handelsbelemmering en moet wetgeving versimpeld en geharmoniseerd worden	een gecoördi-neerde aanpak moet leiden tot een raamwerk voor e-handel; "focus on issues, not on institutions"	bevorderen van marktwerking, consumentenbesche rming, hoge prioriteit voor beveiliging, tegengaan 'identity fraud', brede toegang publiek tot e-handeldiensten

Bijlage II – Samenstelling begeleidingscommissie

prof. mr. T. Heukels, Europa Instituut, Universiteit Leiden (voorzitter)

mr.dr. J.A. Peters, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

mr. H. Hijmans, Ministerie van Justitie

mw. mr. W.M. de Jongste, WODC

Bijlage III – Buitenlandse correspondenten

Georges Chatillon, Université de Paris (Frankrijk)

Christopher Kuner, Morrison & Foerster (Duitsland)

Henry Perritt, Illinois Institute of Technology (VS)

Stephen Saxby, University of Southampton (VK)

Ulrich Sieber, Universität Würzburg (Duitsland)

Bijlage IV
Report of the workshop on internationalisation and jurisdiction, Amsterdam, 29 March 2000

Chairman *Coen Drion* opened the workshop by referring to his bike ride – closing the lock reminded him of the difficulty of solving international legal problems in ICT law. *Jan-Tom Bos* welcomed the participants on behalf of the Dutch Minister of Justice. He outlined the background to the workshop: the Ministry of Justice will present a report to parliament on internationalisation and jurisdiction with respect to ICT law, as a follow-up on the 1998 memorandum *Legislation on the electronic highways*. The workshop is to discuss the main themes of this topic, and it will assess the draft basic rules that will guide Dutch representatives in international negotiations.

Subsequently, *Corien Prins* presented the first conclusions of the comparative study on France, Germany, the UK and the US by Tilburg University that the Ministry of Justice commissioned. The study covers three general themes and four specific subjects, all of which are on the agenda today. The main findings were that governments' preference for self-regulation is increasingly giving way to various forms of co-regulation, that the adage "what holds offline should also hold online" is becoming more difficult to apply as legal problems become more sophisticated, and that enforcement is an issue that, although considered extremely important, governments have no overall solution to. On the specific themes, the research found that governments are largely waiting for the Crime in Cyberspace treaty of the Council of Europe to update judicial co-operation in criminal matters, that the Dutch suggestion to set aside the requirement of double criminality for context-dependent offences has not been discussed abroad, that governments consider the Rome Convention the main way of settling the issue which law applies to online agreements, and that most countries have similar, nationally-centred systems for civil liability of ISPs.

Three general themes and the basic rules

In the morning session, the three general themes and the Ministry's draft basic rules were discussed, each introduced by a participant.

The discussion on **self-regulation**, introduced by *Thomas Smedinghoff*, confirmed the tentative conclusion by Tilburg University that co-regulation is gaining ground. Nevertheless, self-regulation is still important to give the private sector the opportunity to experiment; government interference could hamper innovation. This is particularly stressed in the US, where paradoxically, looking at recent practice, an enormous amount of legislation has been issued (on electronic signatures: 252 laws in 50 states). Moreover, the US private sector increasingly stresses the need for legal certainty, which may call for regulatory steps. Likewise, consumer organisations more and more make themselves heard, asking for government intervention to secure their

interests. These developments have led to the clear US preference for self-regulation shifting towards a tendency to co-regulation, which can better safeguard compelling interests (consumer protection, privacy, legal certainty). The same tendency is seen in France and the UK. The latter country views co-regulation as a partnership in which the government defines minimum conditions. It seems that the exact meaning of the term 'co-regulation' differs in each country.

A useful distinction was made between two types of government intervention: regulation that aims at answering practical questions ("Can I use a digital signature to make a transaction?") and regulation that aims at influencing behaviour ("Don't use encryption that hampers law enforcement!"). The first kind of regulation is generally called for and welcomed by the market, whereas the second kind is generally not favoured.

Of primary importance in the theme of self-regulation is the issue of enforcement. Practice shows that regulation based on voluntary participation can be effective: private parties appear to abide by the rules in order to gain competitive advantages (as in the UK with the official recognition of Certification Authorities).

The discussion on the **adage What holds offline, should also hold online** , introduced by *Corien Prins*, likewise confirmed the finding of Tilburg University that it is becoming increasingly difficult to apply this to specific issues, since it turns out that in order to safeguard the basic principles underlying "offline law" in an online environment, regulations may have to diverge from this starting point. It was felt that the adage was a useful one in the "early days" of ICT law (in the mid 1990s), when it had to be made clear that the Internet was not a legal vacuum. Some participants stressed that we have to look ahead and see what is happening in Cyberspace, rather than stick to this romantic, outdated basic rule. Practice shows that the problems in the online world differ from those in the offline world; in those cases, it is not useful to apply the rules of the offline world.

The most important thing is to identify *why* we have and wish to have certain rules. If we know the goals and rationales of our rule systems and identify the underlying principles, we can analyse to what extent these can hold for both the online and offline worlds. If technology introduces specific differences, we should assess how these affect or should affect the current rules, taking into account the underlying goals of these rules. Rather than rely on transposing traditional rules or principles, governments had perhaps better forget the adage and be simply creative in finding solutions.

It was also pointed out that we have to be aware of the possibility that the adage "what holds offline, should also hold online" may be turned into its reverse: "what holds online, should also hold offline". Thus, the relationship between offline rules and online rules will likely become an interactive one. And, like with self-regulation, a basic issue is the question to what extent the online rules can be enforced.

The third general theme, **enforcement**, introduced by *Bert-Jaap Koops*, had already emerged from the previous discussions as a pivotal issue. This contradicted the research by Tilburg University, which had found very few remarks or ideas in official documents about addressing enforcement of ICT law in an international context as such. This paradox was explained by the comment that governments do think about enforcement a lot, but that they do not have ready-made or overall solutions to it, and consequently refer to it relatively little in official documents.

Various tentative suggestions were made to find ways of safeguarding enforcement. It was felt that finding these ways will depend a lot on the specific problem and the law area. It is easiest to start with areas in which there is a relatively large international agreement on basic principles, such as in the financial-regulations

sector. Also, in private law, where common principles may be found on a multinational or international level, agreements will help ensure enforcement, perhaps through Alternative Dispute Resolution mechanisms. This could take the form of international mediation through national contact points, e.g., by ombudsmen and Chambers of Commerce.

By far the largest enforcement problem is in the area of criminal law. Here, it is less likely to agree upon shared basic principles on an international level, because there are major cultural differences in countries' views on crime and crime fighting. Nonetheless, governments should start on a modest level and see whether agreement can be reached on specific issues that most countries share an interest in, like in combating international financial crimes. Like in private law, international contact points like hotlines could serve as a starting point. It was stressed, however, that addressing international enforcement in criminal law will be a long and slow process.

To finish the morning session, *Hielke Hijmans* presented the Dutch government's **draft basic rules** that will guide Dutch representatives in international negotiations. These basic rules will form a recognisable common position in the many international forums that discuss ICT (self-)regulations, enabling the Netherlands to gain more influence and be more effective, being the small country it is. The draft does not have any official status, but when Parliament accepts the document, the basic rules will become official policy.
The basic rules were viewed as generally uplifting. Some informative questions and critical remarks were made on various details and on the wording of some rules, e.g., on the preference for functional equivalence (it depends on your starting point where this leads you) and on ISP liability (where applying the adage "offline equals online" depends on how you view an ISP).

Specific private-law and criminal-law issues
In the afternoon session, specific private-law and criminal-law issues were discussed in more detail.

Private-law issues*, introduced by Patricia Fry*
As regards private law issues, the discussion in the United States shows that we can distinguish between two lines of reasoning: those who argue that quick action is required for the sake of legal certainty, and those who argue that we first need to understand ICT better before taking any legislative action. In general, one could say that the freedom of contracting should prevail also online, unless this leads to abuse. Contract rules should be default rules instead of minimum standards.

The specific private law topics currently debated in the US are:

- validation of e-contracts
- enforceability of e-contracts
- electronic signatures (including authentication questions)
- data(base) protection
- privacy
- consumer protection
- jurisdiction
- intellectual property.

As regards consumer protection, the consumer organisations tend to lobby for rules that force electronic suppliers to stay in the paper world. Also, arguments are being raised that in order to safeguard consumer protection, new rules for the online world are needed. Thus far, the US government has shown no particular interest in developments outside the US, since the debates raging domestically keep them busy.

As a result, there is no strong push or force that deals with internationalisation of e-commerce issues.

Experience shows that the problems are mitigated once the relevant parties have come to the table to discuss the issues and the special interests.

As regards intellectual-property law, there remains a natural tension between the protection of intellectual-property rights and freedom of information.

As regards private international law issues and cross-border online agreements, no coherent view has emerged so far.

Finally, mention was made of the importance of alternative dispute resolution (ADR) mechanisms. In the US, ADR systems are not seen as favouring consumer interests, because the people involved in the decision-making process are less capable, less informed and often staffed by industry.

The discussion then focused on the United Kingdom. In general, one could say that the UK government takes a 'soft-law approach'. From this perspective, the government takes a special interest in the basic framework of the OECD guidelines on electronic consumer protection. DTI, together with industry, is promoting the introduction of Codes of Conduct.

At present there are no specific initiatives in UK on online consumer protection. The government is closely following the developments on ADR initiatives in the EU.

Although not directly linked to private law, mention was made of an issue that has come up recently in the UK: the relationship between citizens and the government. How far do you allow the citizen to contact the government and what opportunities do you give consumers and businesses to e-contract with the government?

Finally, the discussion showed that there are diverging opinions on the relevance and practicability of a solution for private international law issues by means of 'compartmentalisation'. Such a solution, which uses technological facilities to exclude consumers from jurisdictions with which the supplier does not want to contract, is seen as unrealistic and undesirable in light of technological developments.

***Criminal law issues**, introduced by Stephen Saxby*

The UK Law Commission has given a concise outline of UK law on criminal jurisdiction.[247] "The general rule is that the exercise of criminal jurisdiction does not extend to cover acts committed on land abroad. Jurisdiction over a crime belongs to the country in which it was committed. So, in general, English subjects who commit acts abroad are not amenable to the jurisdiction of the courts in England and Wales. Under the present law, the English courts do not have jurisdiction to try a criminal offence unless the last act or event necessary for its completion occurs within the jurisdiction. This general principle applies to both common law and statutory offences, but as Parliament is supreme it may extend the territorial limit of a particular offence." A good example of the reluctance to laws with extraterritorial effect is the Sexual Offences (Conspiracy and Incitement) Act 1996, which is, inter alia, targeted at sex tourism to the Philippines. It does so by criminalising the preparation for sex-tourism holidays (the preparation takes place in the UK). The government pointed out that there are three reasons for not having laws with extraterritorial effects: (1) criminal law has a territorial base, (2) there are practical difficulties in gathering and

[247] The Law Commission, *Legislating the criminal code: corruption*, Consultation Paper 145, <http://www.lawcom.gov.uk/library/lccp145/cp145.pdf> (visited 30 March 2000), sections 9.2 and 9.3, p. 102, and The Law Commission, *Legislating the criminal code: corruption*, Report 248, <http://www.lawcom.gov.uk/library/lc248/lc248.pdf> (visited 30 March 2000), sections 7.3 and 7.4, p. 105.

presenting in British courts evidence of acts that have occurred abroad, and (3) it is better to have effective laws in the countries where the offences are committed. Therefore, extraterritorial reach should be the exception to the rule. See, e.g., a recent ruling: UK bribery law is not applicable to British executives who bribe foreign officials abroad (Financial Times, 28 March 2000).

An interdepartmental review of the Sexual Offences (Conspiracy and Incitement) Act 1996 has provided some guidelines on when extraterritorial reach of British law might be applied:

a. it concerns serious offences,
b. evidence and witnesses must be likely to be available in the UK,
c. there is international agreement that the conduct in question is reprehensible and that concerted action is needed to deal with the problem,
d. action is needed because of the vulnerability of the victims,
e. action is in the interest of the standing and reputation of the UK in the international community, and
f. there is a danger that if nothing is done, the offenders will not be brought to justice.

It should be stressed that these are not guidelines for the abandonment of double criminality.

What instruments should governments use to enforce criminal law internationally? First of all, there are international conventions, such as the UN Convention on the rights of the child, which was ratified by the UK in 1991. Five years later, this led to the enactment of the Sexual Offences (Conspiracy and Incitement) Act 1996. A drawback of international conventions is that it is second best to improving national laws themselves.

In practice, informal co-operation between enforcement authorities and private organisations – such as the Internet Watch Foundation – in different countries is invaluable. Whether or not this requires (international) regulation is a good question. It is also an open question. As an illustration, one can mention the 'World Wide Sweep for Internet Fraudsters', a surf day organised by the US Federal Trade Commission, in which numerous international organisations participated. The sweep exposed some 1600 suspicious websites (see Financial Times, 24 March 2000).

We ought to be aware of the secondary areas of law that in themselves create the concept of multinational crime. In the UK, taxation law has created problems with regard to the illegal import of cigarettes and spirits. The British government has decided that it wants to increase the monitoring and prosecution of these activities rather than reduce the taxes to a level where the incentive to commit these crime is reduced. That is a perfectly reasonable policy choice for the British government to take.

The discussion took up the issue of the relation between double criminality and extraterritorial jurisdiction. The UK has extraterritorial jurisdiction with respect to offences such as murder, bigamy and child sex. The execution of extraterritorial jurisdiction holds a certain risk of imposing your own norms to foreign countries: a risk that is even more real in a computer network, such as the Internet, that encompasses the entire world. The best solution to this would be a harmonisation of (some?) substantive norms in the field of public-order law. Because such a harmonisation is something that will not happen in the foreseeable future, the requirement of double criminality remains, in principle, a necessary means to avoid imposing a country's own law on foreign countries.

The discussion then addressed the question of whether the requirement of double criminality ought to be met for the crossborder exercise of each and every coercive power, or whether one could discard it for certain powers under certain conditions – in the words of the chairman: "Is there something between black and

white?" There was no discussion about the necessity of the requirement when it comes to extradition or crossborder searches and seizures. There was more discussion over the question whether the requirement has to be met when coercing foreign ISPs to trace and identify Internet users. Although some cases could be envisaged in which such a power without the requirement of double criminality could be useful, the overall opinion was that relinquishing the requirement would "open the floodgates" and make criminal (procedural) law go down the way of censorship. It was pointed out, however, that if a power does not have a coercive element, the requirement need not be met.

Given the idea that a state can not (and may not) impose its norms to a website that is hosted abroad, there could be a shift towards liability of local Internet Access Providers: if they could be required to block access to certain foreign sites, much of the problems surrounding diverging normative claims to the world-wide Internet could be alleviated. The participants declined an obligation to block access to foreign material, because it militates against the very essence of the Internet: the free, uninhibited flow of information. Moreover, blocking measures are costly and probably ineffective.

Overall conclusions

- There is an obvious tendency away from pure market self-regulation in the direction of 'co-regulation', a co-operation by government and business as 'partners' in regulation.
- It is far from clear what exactly should be understood by co-regulation as a starting point. The way this starting is given shape in practice will differ per country, depending on the regulatory tradition. For co-regulation to work in an international context, countries will have to clarify what exactly they take 'co-regulation' to mean.
- In discussing possible government regulation, it is useful to distinguish regulation aiming at influencing behaviour on the one hand, and regulation aiming at answering questions (e.g., to create legal certainty) on the other hand.
- In co-regulation, the government has an obvious task of defining a minimum level of protection and of indicating interests that have to be taken into account.
- The effect of self-regulation and co-regulation will ultimately depend on enforcement: the rules must be enforceable, and they will indeed have to be enforced in practice.
- It is not useful to take rules as a starting point in the adage "what holds offline, should also hold online". Rather, one must identify the (social) function of the rules in the offline world, in order to create rules in the online world that have an analogous function. Resulting rules should thus be functional equivalents.
- The rationale of the adage "what holds offline, should also hold online" lies in creating similar levels of protection in the offline and online worlds. The relationship between offline and online regulation will thus be an interactive process.
- Of primary importance in applying this adage will be the question to what extent enforcement can be sufficiently ensured in the online world. The government will also have to take into account people's trust in the online rules.
- Ultimately, rather than abide by the slightly outdated adage "what holds offline, should also hold online", governments will have to be creative in addressing new problems and issues.
- Enforcement is considered the main problem with respect to ICT law in the international context. However, there are few ideas about safeguarding enforcement in general.

- Enforcement is most likely to be agreed upon in those areas where governments agree upon basic principles, e.g., in the financial sector.
- In private law, enforcement could be safeguarded by international mediation through national contact points (such as ombudsmen or Chambers of Commerce).
- In criminal law, enforcement will be a slow and long process; here also, national contact points can be used to facilitate international enforcement.
- The requirement of double criminality is a fundamental requirement; it is hard if not impossible to find acceptable ways to make exceptions to this.
- The Dutch draft basic rules are welcomed with a fundamentally positive attitude.
- The overall conclusion is that, generally, procedural rules are relatively easy to agree upon (governments and businesses agree how they should agree upon things), whereas substantive rules (reaching specific agreements) are more contentious.

List of participants

Erwin ARKENBOUT	Netherlands	Ministry of Justice
Jan-Tom BOS	Netherlands	Ministry of Justice
Patricia BRUMFIELD FRY	United States of America	Wm. Mitchell College of Law
Georges CHATILLON	France	University of Paris
Lars DAVIES	United Kingdom	London University, Ashurst Morris Crisp
Robbie DOWNING	United Kingdom	Baker & Mc Kenzie
Coen DRION (chairman)	Netherlands	Kennedy van der Laan
Serge GIJRATH	Netherlands	Tilburg University
Nigel HICKSON	United Kingdom	Department of Trade and Industry
Simone VAN DER HOF	Netherlands	Tilburg University
Hielke HIJMANS	Netherlands	Ministry of Justice
Cyril VAN DER NET	Netherlands	Leiden University, Ministry of Justice
Bert-Jaap KOOPS	Netherlands	Tilburg University
Tomas OUDEJANS	Netherlands	Tilburg University
Corien PRINS	Netherlands	Tilburg University
Stephen SAXBY	United Kingdom	University of Southampton
Maurice SCHELLEKENS	Netherlands	Tilburg University
Florence SCHMIDT-PARISET	France	OECD, Ministry of Justice
Thomas SMEDINGHOFF	United States of America	Baker & Mc Kenzie
Guido TIELMAN	Netherlands	Ministry of Foreign Affairs
Frederique VAN ZOMEREN	Netherlands	Ministry of Justice

Auteurs

De auteurs zijn allen werkzaam bij het Centrum voor Recht, Bestuur en Informatisering (CRBI) van de Katholieke Universiteit Brabant.

Serge Gijrath
Mr. drs. Serge Gijrath is advocaat te Amsterdam, partner bij Caron & Stevens/Baker & McKenzie, en hij is sinds 1999 onderzoeker bij het CRBI. Hij is gespecialiseerd in de juridische aspecten van informatietechnologie en telecommunicatie, met als sub-specialisatie intellectueel-eigendomsrecht.

Bert-Jaap Koops
Dr. Bert-Jaap Koops is sinds 1998 postdoc bij het CRBI. Hij studeerde wiskunde en algemene literatuurwetenschap in Groningen en werkte van 1994-1998 als AIO aan de KUB en de Technische Universiteit Eindhoven. In januari 1999 promoveerde hij op het proefschrift *The Crypto Controversy*. Koops doet onderzoek op het gebied van recht en informatietechnologie, in het bijzonder strafvordering en ICT, computercriminaliteit, encryptie, digitale handtekeningen en TTP s. In 2000-2001 richt hij zich op het grensvlak tussen strafvordering en privacy onder invloed van ICT, met een persoonsgerichte subsidie van NWO.

Corien Prins
Prof. mr. Corien Prins is sinds 1994 hoogleraar Recht en Informatisering bij het CRBI. Zij studeerde vanaf 1980 Slavische Taal en Letterkunde en Rechtsgeleerdheid aan de Rijksuniversiteit Leiden, waar zij in 1991 promoveerde. Zij doceerde in 1993 als *invited visiting professor* aan de Hastings School of Law (University of California, San Francisco). Prins is redactielid van diverse nationale en internationale tijdschriften en losbladige uitgaven. In haar onderzoek concentreert zij zich momenteel op elektronische handel, privacy en anonimiteit, agents en reguleringsuitgangspunten inzake ICT.

Maurice Schellekens
Mr. ir. Maurice Schellekens is sinds 1999 postdoc bij het CRBI. Daarvoor was hij assistent in opleiding bij dit Centrum. Eind 2000 verschijnt zijn dissertatie over de aansprakelijkheidspositie van Internet-intermediairen in het strafrecht en het auteursrecht. In 1999 verscheen van zijn hand een ITeR-studie naar strafbare feiten op de elektronische snelweg. Maurice Schellekens studeerde Nederlands Recht aan de Rijksuniversiteit Maastricht en Technische Informatica aan de Technische Universiteit Eindhoven.

Eric Schreuders
Mr. Eric Schreuders is sinds 1996 onderzoeker bij het CRBI. In het kader van het nationaal programma voor Informatietechnologie en Recht (ITeR) bereidt hij bij het CRBI een dissertatie voor over de juridische aspecten van knowledge discovery in databases (KDD) en data mining. Hij geeft doctoraal- en PAO-onderwijs op het gebied van privacy.